"DISEÑO DE UN PLAN DE RECUPERACIÓN EN CASO DE DESASTRES PARA LA PLATAFORMA INFORMÁTICA DE RECAUDOS Y CONTROL DE FLOTA DE UN SISTEMA DE TRANSPORTE MASIVO DE PASAJEROS"

EMPRESA ESTUDIO
"RECAUDOS SIT BARRANQUILLA S.A.S."

MISAEL ALONSO NIÑO ALVAREZ

Proyecto de grado para optar por el título de Magíster en Gobierno de Tecnología Informática

Tutor
Dr. WILSON NIETO BERNAL,
DOCTOR EN TECNOLOGÍAS DE LA INFORMACIÓN
División de Ingenierías

UNIVERSIDAD DEL NORTE
MAESTRIA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
DIRECCIÓN DE PROYECTOS TELEMATICOS
BARRANQUILLA – ATLÁNTICO
2017

Contenido

LISTA DE FIGURAS

1. INTRODUCCIÓN

En la actualidad, es un hecho que la gran mayoría de los procesos de negocios son soportados, automatizados y gestionados por sistemas de información que apoyan la actividad gerencial en la toma de decisiones; incluso muchas veces, tratar de tener acceso a los sistemas de información o acceso a la propia información y no poder obtenerlo se puede considerar un desastre

Un Desastre en una organización puede considerarse entre otras cosas, como la pérdida de datos, el no tener acceso a la información, un desastre natural que destruya la plataforma tecnológica, cualquier evento no planeado que cause la interrupción de la operación normal del negocio se considera un desastre y tener un sólido plan de recuperación de desastres es la clave para lograr que el negocio vuelva a funcionar con muy poco o ningún tiempo de inactividad. El presente documento está enfocado al diseño de un plan de recuperación de desastre para la plataforma informática de recaudos y control de flota de un sistema de transporte masivo de pasajeros controlado por la compañía Recaudos SIT Barranquilla S.A.S. por consiguiente se realiza una breve descripción de esta.

RECAUDOS SIT Barranquilla S.A.S, es una compañía colombiana constituida como Concesionaria para la operación y explotación del sistema de Recaudo y el suministro del Sistema de gestión y Operación del Sistema Integrado de Transporte masivo de Pasajeros del Distrito de Barranquilla y su área Metropolitana, es el principal aliado tecnológico de **Transmetro S.A.S.**, brindando experiencia y su infraestructura humana, tecnológica y operativa, para la operación de la concesión, bajo los mayores estándares de calidad y seguridad.

Misión

Recaudos SIT Barranquilla es una compañía dedicada a la prestación de soluciones tecnológicas y el recaudo del sistema de transporte masivo, que mediante la utilización de tecnología adecuada y un equipo humano Altamente calificado, logra desarrollar soluciones integrales de alta calidad, generando valor para sus accionistas, proveedores, clientes, trabajadores y comunidad. [1]

Visión

Para el 2020 Recaudos SIT Barranquilla S.A. estará posicionado como líder de la región Caribe en la prestación de soluciones tecnológicas y recaudo de los sistemas de transporte Masivo de Pasajeros, siendo reconocida por su capacidad para desarrollar soluciones integrales, la confiabilidad de sus procesos y el compromiso con el bienestar y desarrollo de su talento humano. [2]

2. PLANTEAMIENTO DEL PROBLEMA

El contrato de Concesión entre la firma reguladora y la empresa Concesionaria para la operación, explotación del Sistema Integrado de Transporte masivo de Pasajeros y de Recaudos del Distrito de Barranquilla y su área Metropolitana, exige que el sistema esté disponible en un 98.6 % durante la operación diaria y en caso de presentarse un siniestro, el servicio se debe restablecer en un tiempo menor a 90 minutos. Debido a las exigencias mencionadas anteriormente y al no cumplimiento de estos términos, el ente gestor del contrato de concesión, podrá colocar las multas que estime necesario de acuerdo al capítulo de multas [3]

2.1 ANTECEDENTES

En los comités de Gerencia y Técnicos se han expuesto e identificado fallas inesperadas en los diversos subsistemas que causan la no continuidad del servicio de recaudos o de control de flota, estas pueden ser por: Fallas por problemas con el fluido eléctrico, fallas por inundaciones causadas por lluvias y arroyos, fallas por el sistema de control ambiental en los data center, fallas ocasionadas por vandalismo o desordenes de orden público en las estaciones, fallas por actualización de software de terceros, también se ha indagado con especialistas de Transportes masivos que vienen de otras ciudades a realizar visitas técnicas o auditorias contratadas por el ente gestor, expresando que no conocen o no se tiene la información de que existan planes de recuperación de desastres informáticos enfocados en otros sistemas de transporte masivo, pero si algunos planes de contingencia sencillos, lo que hace necesario, tener un plan de Recuperación de Desastres, para poder minimizar el riesgo que se tiene debido a las fallas anteriormente mencionadas.

2.2 PREGUNTA PROBLEMA

¿Cómo lograr que la plataforma tecnológica del Sistema de Recaudos y de Control de Flota esté disponible en un 98,6% durante la operación diaria y si se presenta un incidente este sea resuelto en un tiempo menor a 90 minutos?

2.3 JUSTIFICACIÓN

El diseñar un plan de recuperación de desastres para la Plataforma tecnológica del sistema informático de recaudos y control de flota de la Empresa Recaudos SIT Barranquilla S.A.S. ayudara minimizar el impacto operacional y económico, cada vez que surja, un incidente, una falla o un desastre al sistema informático, debido a que se disminuirá el riesgo de no cumplir con los lineamientos de los acuerdos de los niéveles de servicio que exige el contrato de concesión entre la firma reguladora y la empresa concesionaria. [4]

El plan de recuperación de desastres ayudará a restablecer el servicio en un tiempo menor al máximo permitido, también garantizará la continuidad del servicio en el porcentaje exigido a la operación diaria. [5]

Con el diseño del plan de recuperación de desastres, se logrará minimizar varios riesgos y se pueden mencionar los siguientes: el primer riesgo que se evitaría, seria por multas, que impondría la empresa reguladora del sistema de Transporte Masivo de Pasajeros al no cumplir con los lineamientos de los niveles de Servicios contratados; el segundo es por devolución de pasajes a usuarios del sistema, el tercero, a nivel operativo al mover empleados en sus turnos de trabajo, extendiendo sus jornadas laborales habituales, para cubrir o solucionar fallas al sistema, otros aspectos también seria la reducción de altos costos por la compra de componentes de Hardware descompuestos, reducir costos por la renovación o adquisición de nuevas licencias de software que garanticen la estabilidad de la plataforma, altos costos por la adquisición de componentes de hardware que garanticen la continuidad del servicio.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un plan de recuperación en caso de desastres, para la plataforma informática de recaudos y control de flota de un sistema de transporte masivo de pasajeros, tomando como base la empresa Recaudos SIT Barranquilla S.A.S. Para que cada vez que ocurra un incidente que afecte la operación del sistema, se garantice la recuperación oportuna y la continuidad del servicio del sistema informático.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar las metodologías y mejores prácticas que se deben tener en cuenta para poder aplicar un plan de Recuperación de Desastres a la empresa concesionaria del sistema Integrado de Transporte masivo de Pasajeros y de Recaudos del Distrito de Barranquilla y su área Metropolitana.

- Diseñar la guía que permita crear el plan de recuperación de desastres, enfocado a incidentes de tipo natural, informático o humano, para que pueda ser ejecutado por el personal técnico de la empresa y se pueda restablecer el servicio antes del tiempo contractual exigido por el contrato de concesión.

- Crear el plan de recuperación de desastres para que en el evento de presentarse un incidente sobre los sistemas de Recaudos o de control de flota, se apliquen las recomendaciones del plan y el servicio se pueda restaurar en un tiempo menor a 90 minutos.

4. ALCANCES Y LIMITACIONES DEL PROYECTO

4.1 ALCANCES

Elaborar un Plan de Recuperación podría decirse que es una disciplina que prepara a la organización para poder continuar operando durante un incidente que afecte su operación. Este plan contemplara los procedimientos y planes de contingencia, que se realizarán para dar continuidad a la Plataforma tecnológica del sistema informático de recaudos y control de flota de la Empresa Recaudos SIT Barranquilla S.A.S.

El Plan de Recuperación de Desastres incluirá los aspectos y tareas más representativas que deberán ejercer La Gerencia General, La Gerencia Técnica operativa, la Dirección de Mantenimiento y la Dirección de Gestión e Información de la Empresa Recaudos SIT Barranquilla S.A.S. para enfrentar situaciones que amenacen o afecten la integridad de la Plataforma tecnológica del sistema informático de recaudos y control de flota. [6]

Los incidentes a tener en cuenta y que se trabajarán en el Plan de Recuperación de Desastres son, riesgos asociados a problemas eléctricos, riesgo por incendio, riesgo por filtraciones de agua o inundaciones, riesgo por problemas de desorden público y riesgo por errores humanos, los cuales se detallarán en el análisis de riesgos que se presenta más adelante.

4.2 LIMITACIONES

Las Tareas y acciones del plan de Recuperación de desastres será aplicado a la Plataforma tecnológica del sistema informático de recaudos y control de flota de la Empresa Recaudos SIT Barranquilla S.A.S. en sus dos data center y en estaciones de que conforman las paradas de buses de Transmetro de la Calle Murillo y la Carrera 46 de la ciudad de Barranquilla.

5. ESTADO DEL ARTE

Una de las primeras etapas a desarrollarse dentro de este proyecto es la construcción de su estado del arte, ya que permite determinar la forma como ha sido tratado el tema de Planes de Recuperación de Desastres (**DRP**) en otras empresas, cómo se encuentra el nivel de su conocimiento en el momento de realizar esta investigación y cuáles son las tendencias y propuestas existentes, es por esto que el estado del arte, se basara en las siguientes premisas; Tema, fuentes, Antecedentes, Experiencias e Ideas

Figura No 1: Estado del Arte
Fuente: Elaboración Propia

5.1 TEMA: PLAN DE RECUPERACIÓN DE DESASTRES (DRP - DISASTER RECOVERY PLAN)

Un Desastre en una empresa pude ser muchas cosas, podría decirse que un desastre es un evento que imposibilita la continuación de las funciones normales de la empresa, desde un desastre natural, que destruya toda la plataforma informática de la empresa o cualquier evento que cause la interrupción en la operación normal del negocio, un plan de recuperación de desastres se compone de las precauciones tomadas para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente funciones de misión crítica. Por lo general, la planificación de recuperación de desastres implica un análisis de los procesos de negocio y las necesidades de continuidad, sin un plan de recuperación de desastres a la mayoría de las empresas que les ocurre esto no se recuperan, generalmente quedan en pérdida total y en banca rota. [7]

5.2 FUENTES

Estudios pilotos y experiencias vividas con los diferentes sucesos que puedan afectar la continuidad del negocio debido a la ocurrencia de un desastre y que no se tenga establecido un plan de recuperación para solucionar el incidente.

DRI: Disaster Recovery Institute; organización sin ánimo de lucro que proporciona formación a nivel internacional como organismo de certificación de profesionales para la Gestión de la Continuidad de Negocio. DRI establece estándares profesionales para la planificación de la continuidad del negocio [8]

TECHTARGET: proporciona estrategias tecnológicas para los profesionales de las TI. Ofrecen consejos, estrategias y mejores prácticas en el ámbito tecnológico que le ayudarán a simplificar y racionalizar sus operaciones.

Grupo Albe: Es una empresa de consultoría que cuenta con consultores e instructores que en sus servicios de consultoría a diseñado una metodología para implementar **DRP** *(Disaster Recovery Plan) (Plan de Recuperación de Desastres) a* proyectos de consultoría con sus clientes. [9]

IBM: International Business Machines, empresa multinacional estadounidense de tecnología y consultoría con sede en Armonk, Nueva York. IBM fabrica y comercializa hardware y software para computadoras y ofrece servicios de infraestructura, alojamiento de Internet y consultoría en una amplia gama de áreas relacionadas con la informática. [10]

IBM Knowledge Center - Centro de conocimientos de IBM: Blogs de Especialistas de IBM donde aportan y comparten sus experiencias en diversas áreas de la Tecnología así como metodologías y ejemplos para un DRP [11]

VMware: Es una compañía que proporciona software de virtualización disponible para ordenadores compatibles X86. También es una filial de EMC Corporation (propiedad a su vez de Dell Inc) [12]

Blogs Vmware: Blogs de Especialistas de VMware donde comparten sus experiencias en diversas áreas de la Tecnología de la virtualización así como ejemplos para un DRP [13]

BOSTON Computing Network: Empresa de servicios técnicos de outsourcing, asus clientes, dentro de los servcios que propone esta Web Hosting, Consultoría en Tecnologías Informáticas y desarrollo web [14]

5.3 ANTECEDENTES

Los Planes para dar continuidad a una actividad de negocio no son nuevos, la mayoría de empresas que poseen plan de recuperación de desastres buscan como primera acción, evitar el riesgo, con planes de acción, capacitación a personal de planta, de tal manera que todos en la compañía sepan que deben hacer y cómo actuar en caso de un desastre, luego de que gran parte del riesgo está cubierto, también buscan transferirlo a compañías aseguradoras para que sus activos no se pierdan totalmente en caso de un desastre.

Según los datos reportados en Grupo ALBE, algunas de las causas de las pérdidas de datos son debido a:

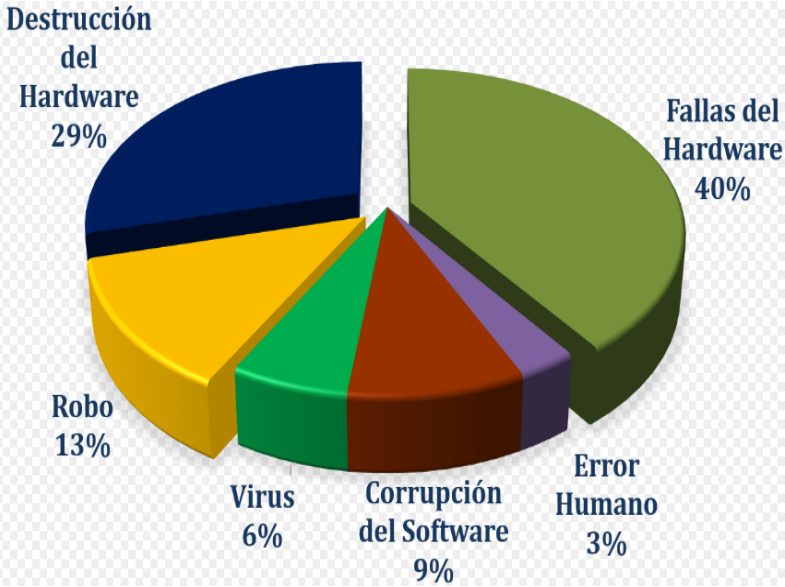


Figura No 2: Pérdidas de Datos
Fuente: Grupo Albe

Otra estadística por la **BOSTON Computing Network** menciona lo siguiente:

- 6% las pc's sufren algún evento de pérdida de datos en cualquier año.
- 30% de todas las empresas que tienen un incendio importante de salir del negocio dentro de un año. 70% fallan dentro de cinco años. (Home Office Computing Magazine)
- El 31% de los usuarios de PC´S han perdido todos sus archivos debido a eventos fuera de su control.
- El 34% de las empresas no puede probar sus copias de seguridad en cinta, y de las que lo hacen, el 77% ha encontrado fallos de respaldo de cinta.
- 60% de las empresas que pierden sus datos cerrarán dentro de los siguientes 6 meses después del desastre.
- El 60% de las empresas que pierden sus datos se cerrará dentro de los 6 meses del desastre.
- 93% de las empresas que perdieron su centro de datos durante 10 días o más debido a un desastre se declaró en quiebra en el plazo de un año del desastre
- Las empresas que no son capaces de reanudar sus operaciones dentro de los diez días siguientes a un desastre, no es probable que sobrevivan.
- Cada semana 140,000 discos duros dejan de funcionar en los Estados Unidos.

Para reducir estos eventos y controlarlos hasta cierto grado, se hace necesaria la intervención del Equipo de Evaluación de Desastres o en su efecto de un Comité de Riesgos: esta entidad interna será la que evaluará los daños de los activos físicos y de las capacidades funcionales del centro

de datos en la eventualidad de un desastre, para posteriormente emitir un reporte al Equipo Ejecutivo, el cual en conjunto con otra información disponible tomará la decisión respecto a la declaratoria formal del desastre.

5.4 EXPERIENCIAS

Dentro de la compañía se establece como política sacar indicadores mensuales de los dispositivos que sufren fallas y el tipo de fallas que generan no continuidad en el servicio que presta el dispositivo, para lo cual se hace una evaluación de indicadores mensual donde se revisa si se está o no cumpliendo con los niveles de servicio acordados en el contrato de concesión del Transporte Masivo, para dispositivos de recaudos, servidores y Switch de comunicaciones de la plataforma tecnológica que soporta la operación del Transporte Masivo

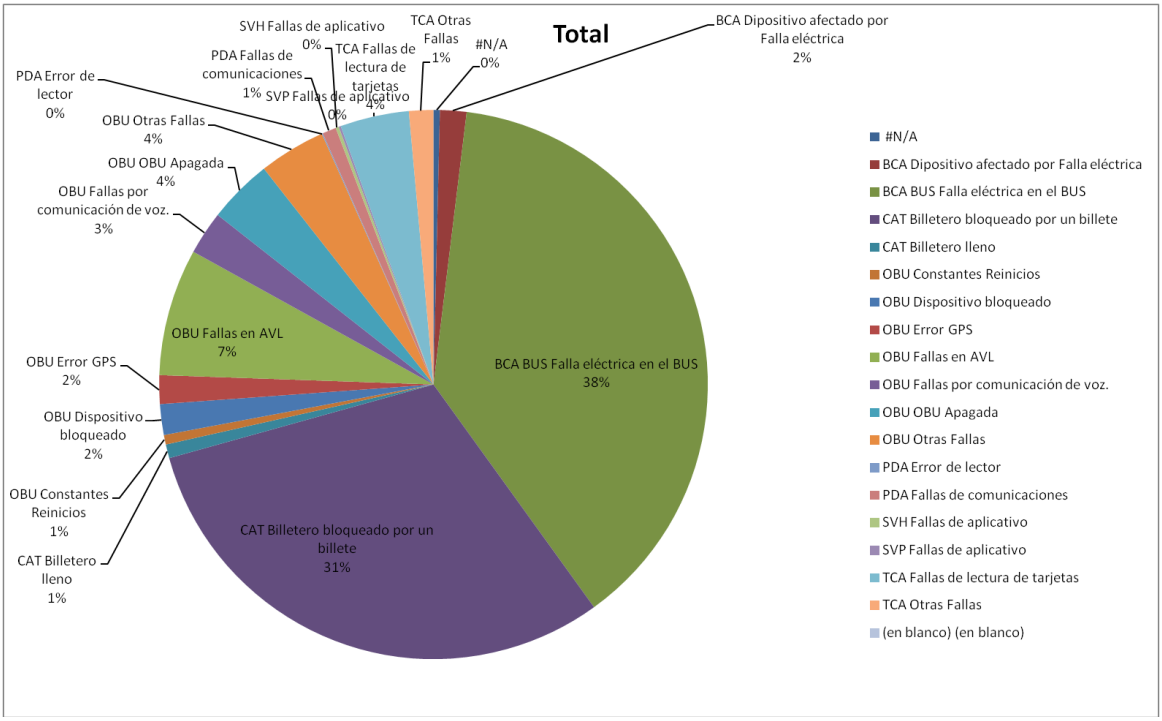
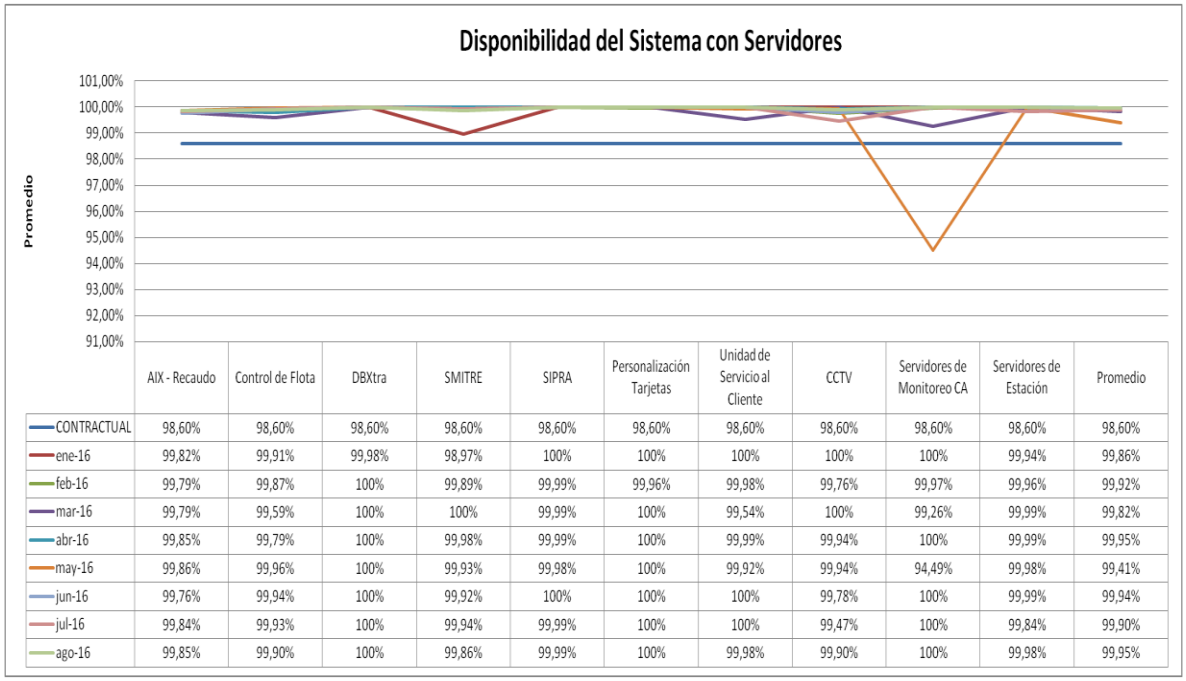
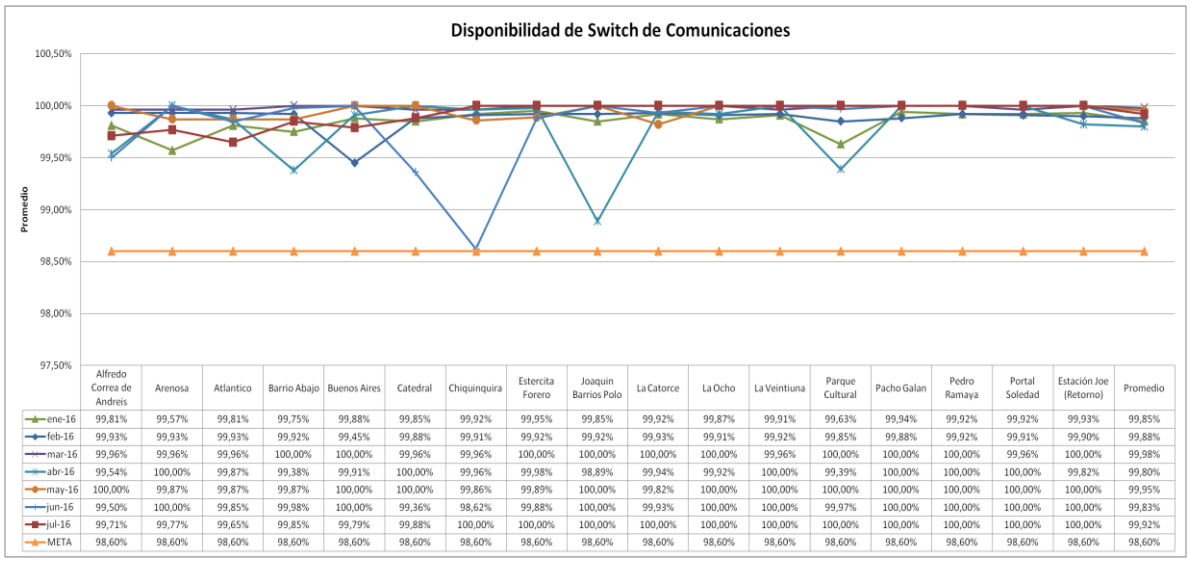


Figura No 3: Fallas que se presentan en los dispositivos de Recaudos
Fuente: Plataforma de Gestión – Recaudos SIT



	AIX - Recaudo	Control de Flota	DBXtra	SMITRE	SIPRA	Personalización Tarjetas	Unidad de Servicio al Cliente	CCTV	Servidores de Monitoreo CA	Servidores de Estación	Promedio
CONTRACTUAL	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%
ene-16	99,82%	99,91%	99,98%	98,97%	100%	100%	100%	100%	100%	99,94%	99,86%
feb-16	99,79%	99,87%	100%	99,89%	99,99%	99,96%	99,98%	99,76%	99,97%	99,96%	99,92%
mar-16	99,79%	99,59%	100%	100%	99,99%	100%	99,54%	100%	99,26%	99,99%	99,82%
abr-16	99,85%	99,79%	100%	99,98%	99,99%	100%	99,99%	99,94%	100%	99,99%	99,95%
may-16	99,86%	99,96%	100%	99,93%	99,98%	100%	99,92%	99,94%	94,49%	99,98%	99,41%
jun-16	99,76%	99,94%	100%	99,92%	100%	100%	100%	99,78%	100%	99,99%	99,94%
jul-16	99,84%	99,93%	100%	99,94%	99,99%	100%	100%	99,47%	100%	99,84%	99,90%
ago-16	99,85%	99,90%	100%	99,86%	99,99%	100%	99,98%	99,90%	100%	99,98%	99,95%

Figura No 4: Disponibilidad del Sistema con Servidores
Fuente: Plataforma de Gestión – Recaudos SIT



	Alfredo Correa de Andreis	Arenosa	Atlantico	Barrio Abajo	Buenos Aires	Catedral	Chiquinquira	Estercita Forero	Joaquin Barrios Polo	La Catorce	La Ocho	La Veintiuna	Parque Cultural	Pacho Galan	Pedro Ramaya	Portal Soledad	Estación Joe (Retorno)	Promedio
ene-16	99,81%	99,57%	99,81%	99,75%	99,88%	99,85%	99,92%	99,95%	99,85%	99,92%	99,87%	99,91%	99,63%	99,94%	99,92%	99,92%	99,93%	99,85%
feb-16	99,93%	99,93%	99,93%	99,92%	99,45%	99,88%	99,91%	99,92%	99,92%	99,93%	99,91%	99,92%	99,85%	99,88%	99,92%	99,91%	99,90%	99,88%
mar-16	99,96%	99,96%	99,96%	100,00%	100,00%	99,96%	99,96%	100,00%	100,00%	100,00%	100,00%	99,96%	100,00%	100,00%	100,00%	99,96%	100,00%	99,98%
abr-16	99,54%	100,00%	99,87%	99,38%	99,91%	100,00%	99,96%	99,98%	98,89%	99,94%	99,92%	100,00%	99,39%	100,00%	100,00%	100,00%	99,82%	99,80%
may-16	100,00%	99,87%	99,87%	99,87%	100,00%	100,00%	99,86%	99,89%	100,00%	99,82%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,95%
jun-16	99,50%	100,00%	99,85%	99,98%	100,00%	99,36%	98,62%	99,88%	100,00%	99,93%	100,00%	100,00%	99,97%	100,00%	100,00%	100,00%	100,00%	99,83%
jul-16	99,71%	99,77%	99,65%	99,85%	99,79%	99,88%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,92%
META	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%	98,60%

Figura No 5: Disponibilidad de Switch de Comunicaciones
Fuente: Plataforma de Gestión – Recaudos SIT

5.5 IDEAS

Dado las condiciones del sistema de Transporte masivo de pasajeros y debido a las exigencias contractuales de mantener un nivel de disponibilidad bien alto, (98,6 % de Disponibilidad) y solucionar los inconvenientes en un tiempo menor

a 90 minutos surge una idea base, que para mantener este sistema, cumpliendo con los lineamientos contractuales y los desastres que normalmente ocurren, y que afectan la operación y el nivel de disponibilidad surge la idea de Implementar un **DRP**[1] Dentro de la compañía administradora de la plataforma tecnología del sistema de Recaudos y Control de Flota, del sistema de Transporte masivo de pasajeros. El plan de recuperación de desastres se compone de las precauciones tomadas para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente las funciones de misión crítica.

6. MARCO DE REFERENCIA

El presente trabajo de titulación propone un marco de Referencia para un **DRP *(Disaster Recovery Plan) Plan de Recuperación de Desastres.*** *S*e basa en las mejores prácticas establecidas por los profesionales o entidades de la recuperación de desastres a nivel mundial, como lo es "***DRI: Disaster Recovery Institute"***, a su vez partiendo de las mejores prácticas o estándares de la industria que sustentan el **DRP,** tomando como referencias de **"ISACA -** ***Information Systems Audit and Control Association*** **- Asociación de Auditoría y Control de Sistemas de Información** ***"***; el marco de Trabajo de ***COBIT-5***[2] ***– " Proceso DSS04: Gestionar la Continuidad"*** también, aplicando aspectos de la norma ***"Norma ISO 22301 – Gestión de la continuidad de Negocio***; [15] las mejores prácticas que recomienda "***ITIL, (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de Información"*** [16] para la gestión de servicios de T.I. y las metodologías recibidas en las clases de la Maestría de Gobierno de T.I. basadas en **"E*l Comité de Normas Conjuntas Australia / Nueva Zelanda AS / NZS 4360 Gestión de Riesgos"*** para la evaluación y tratamiento de los riesgos en los que incurre un proyecto de Tecnologías Informáticas.

[1] **DRP *(Disaster Recovery Plan) Plan de Recuperación de Desastres.***
[2] ***COBIT-5****: Se lanzó el 10 de abril de 2012 por ISACA,* ***COBIT-5*** *es la última edición, la cual proporciona una visión empresarial del Gobierno de TI y la Gestión de la TI de la empresa que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas*

7. MARCO TEÓRICO

7.1 NORMAS APLICADAS AL DRP

7.1.1 COBIT 5

Es un modelo de referencia que describe 34 procesos relacionados con TI y que son comunes a todas las organizaciones. Cada proceso está descrito en detalle, incluyendo entradas y salidas, actividades clave, objetivos, indicadores de desempeño y un modelo básico de madurez. Fue creado por la organización ISACA[3], para el proyecto del DRP se escogió la versión de COBIT 5 y este marco de Gobierno de TI y Gestión de TI de la empresa se basa en cinco principios

Principio 1: Satisfacer las Necesidades de las Partes Interesadas-Stake Holders
Principio 2: Cubrir la Empresa Extremo-a-Extremo
Principio 3: Aplicar un Marco de Referencia Único Integrado
Principio 4: Hacer Posible un Enfoque Holístico
Principio 5: Separar el Gobierno de la Gestión

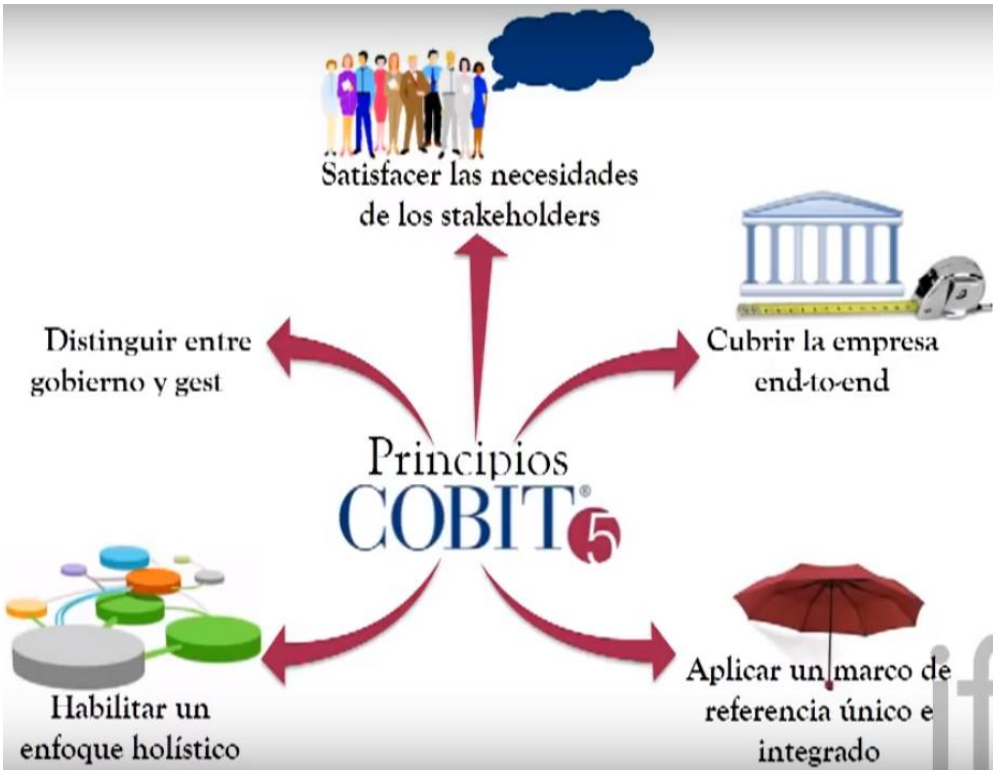


Figura No 6: Principios de COBIT 5
Fuente: https://www.youtube.com/watch?v=V4ONzLrfoK8

[3] ***ISACA****: es el acrónimo* de ***Information Systems Audit and Control Association - (Asociación de Auditoría y Control de Sistemas de Información*** Esta asociación apoya el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

7.1.1.1 Proceso DSS04: Gestionar la Continuidad

Este Proceso da las pautas para Establecer y mantener un plan que permita al negocio y a TI responder a incidentes e interrupciones de servicio, para que la operación continua de los procesos críticos del negocio y los servicios TI requeridos logren mantener la disponibilidad de la información a un nivel aceptable para la empresa, ante el evento de una interrupción significativa.

7.1.2 ITIL[4], Biblioteca de Infraestructura de Tecnologías de Información

ITIL. Es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios, el desarrollo y las operaciones relacionadas con las tecnologías de la información.

ITIL divide el ciclo de vida de un servicio en 5 fases

Fase 1: ***Estrategia del servicio***, cuyo propósito es definir qué servicios se prestarán, a qué clientes y en qué mercados

Fase 2: ***Diseño del servicio***, responsable de desarrollar nuevos servicios o modificar los ya existentes, asegurando que cumplen los requisitos de los clientes y se adecuan a la estrategia predefinida

Fase 3: ***Transición del servicio***, encargada de la puesta en operación de los servicios previamente diseñados

Fase 4: ***Operación del servicio***, responsables de todas las tareas operativas y de mantenimiento del servicio, incluida la atención al cliente

Fase 5: ***Mejora continua del servicio***, a partir de los datos y experiencia acumulada propone mecanismos de mejora del servicio

[4] ***ITIL, (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de Información***

7.1.3 ANALISIS DE RIESGOS

Metodologías recibidas en las clases de la Maestría de Gobierno de T.I. con base a ***"El Comité de Normas Conjuntas Australia / Nueva Zelanda AS /NZS 4360 Gestión de Riesgos"*** **[17]** para la evaluación y tratamiento de los riesgos en los que incurre un proyecto de Tecnologías Informáticas.

El estándar **AS/NZS 4360**[5] Provee una guía genérica para el establecimiento e implementación para el proceso de administración de riesgos, involucrando el contexto, la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo de los riesgos, de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades.

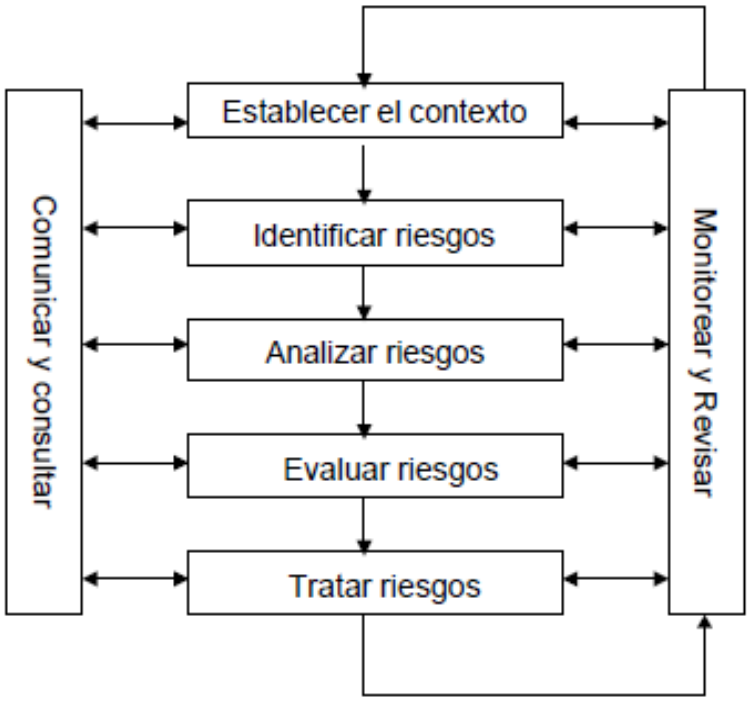


Figura No 7: Vista General de la Administración de Riesgos
Fuente: Estándar Australiano **AS/NZS 4360**

[5] El estándar **AS/NZS 4360:** ***Comité de Normas Conjuntas de Australia / Nueva Zelanda AS / NZS 4360 para la Gestión de Riesgos***

7.1.4 GESTIÓN DE LA CONTINUIDAD DE NEGOCIO - NORMA ISO 22301[6]

Es una norma internacional de gestión de continuidad de negocio. Esta norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando.

La norma ISO 22301 está organizada de acuerdo a la siguiente estructura:

1) **Ámbito de aplicación**.
2) **Referencias normativas**.
3) **Términos y definiciones**.
4) **Contexto de la organización**: Consiste en identificar el alcance del **SGCN**[7], teniendo en cuenta los objetivos estratégicos de la organización, sus productos y servicios claves, su tolerancia al riesgo, así como cualquier obligación reglamentaria.
5) **Liderazgo**: La alta dirección debe demostrar un compromiso continuo con el SGCN. A través de su liderazgo y acciones, la dirección puede crear un ambiente en el cual el personal esté completamente involucrado y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización.
6) **Planificación**: Se establecen objetivos estratégicos y principios para la orientación del SGCN en su totalidad.
7) **Soporte:** La gestión diaria de un Sistema de Gestión de la Continuidad de Negocio, se basa en el uso de los recursos apropiados para cada actividad. Estos recursos incluyen personal competente, toma de conciencia y comunicación, etc. todo esto debe estar apoyado por la documentación que sea necesaria.
8) **Operación Después de la planificación del SGCN**: La organización debe ponerlo en funcionamiento.
9) **Evaluación del desempeño**. La norma **ISO 22301** requiere un seguimiento permanente del sistema, así como revisiones periódicas para mejorar su operación.
10) **Mejora**: La organización puede mejorar continuamente la eficacia de su sistema de gestión a través del uso de la política de **continuidad de negocio**, los objetivos, los resultados de auditorías, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección

[6] **Norma *ISO 22301*** *- Norma Internacional para la Gestión y continuidad de Negocio*
[7] ***SGCN - Sistema de Gestión de la Continuidad de Negocio***

Esta Norma aplica a todos sus procesos la Estructura de Planear, Hacer, Verificar y Actuar

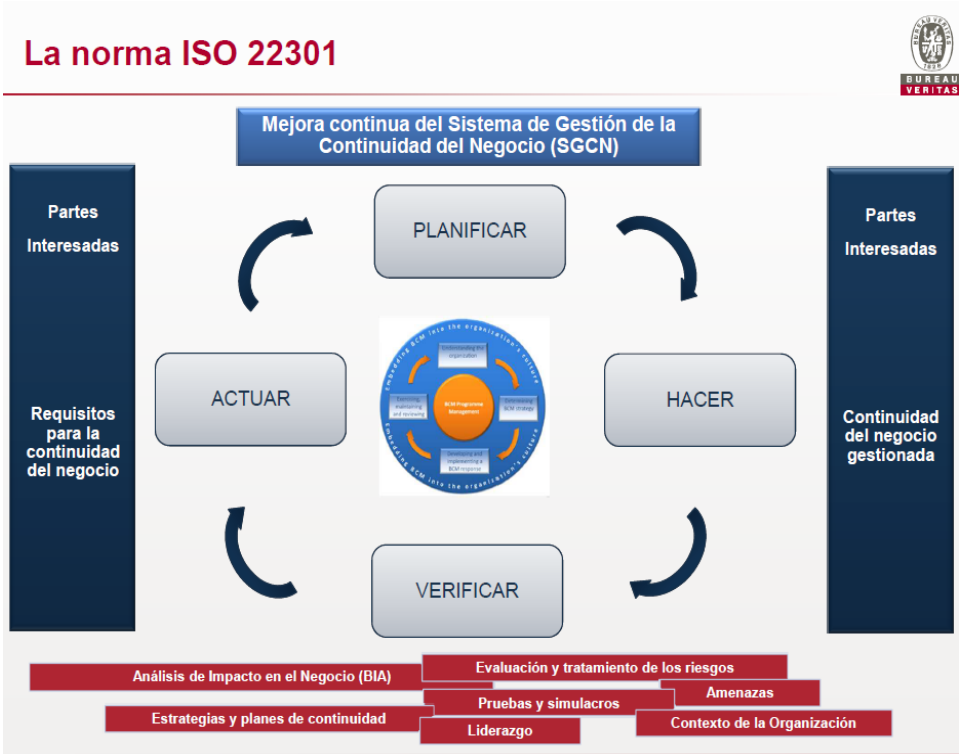


Figura No 8: Norma ISO 22301
Fuente: http://www.bureauveritas.es/

7.2 CONCEPTOS DE RECUPERACIÓN DE DESASTRES QUE SE DEBEN CONOCER

7.2.1 RECUPERACIÓN DE DESASTRES

Es la parte del plan de seguridad que se encarga de proteger a una organización de un incidente negativo. Ese acontecimiento negativo podría ser algo relacionado con los equipos de cómputo, un virus informático, un desastre natural como un incendio o un terremoto. Un plan de recuperación de desastres es lo que las empresas utilizan para volver al servicio después de la catástrofe. Se crea el plan para minimizar el efecto del evento negativo. Su objetivo debe ser limitar el efecto de la catástrofe y permitir que la empresa continúe de manera normal tan pronto como sea posible.

7.2.2 CONMUTACIÓN POR ERROR, O FAILOVER

Este concepto se refiere a un modo de operación de respaldo que se utiliza cuando el sistema primario no está disponible. Un sistema secundario toma el control de ciertos componentes, tales como un servidor, la red, la Base de Datos y cuando el sistema primario falla el

sistema secundario mantiene el servicio, La conmutación por error es muy importante para los sistemas de misión crítica que necesitan funcionar constantemente y trabajar incluso después de un desastre.

7.2.3 PUNTO DE RECUPERACIÓN

El objetivo del punto de recuperación es la máxima cantidad de tiempo que puede tardar la recuperación de archivos del almacenamiento del sistema de copias de seguridad para reanudar las operaciones de manera normal después de un desastre. También determina la frecuencia con la que se deben crear los archivos de copia de seguridad.

7.2.4 TIEMPO DE RECUPERACIÓN

Es una parte vital de la recuperación de desastres. Es la máxima cantidad de tiempo que un equipo de cómputo, un sistema de información, una aplicación o una red puede estar inactiva después de que ocurre un desastre o falla. Básicamente, es el tiempo deseado para que todo esté de nuevo en marcha después de que sucede un desastre

7.2.5 REPLICACIÓN

La **replicación** es el proceso de copiar y mantener actualizados los datos en varios nodos. Éste usa un concepto donde existe un nodo maestro y otros esclavos. La replicación es el proceso mediante el cual se genera una **copia exacta** de parte del sistema, de un nodo A, hacia un Nodo B

8. METODOLOGÍA PARA EL DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES

8.1 ESCENARIO DE SITUACIÓN

- Cada día nuestra economía global se está volviendo más compleja
- Los incidentes que ocurren en nuestro negocio o entorno pueden frenar o incluso paralizar nuestra actividad, impactando directamente en nuestros clientes y en los procesos críticos del negocio, esto especialmente se puede dar en sectores como: TICs, administración pública, financiero e industrial.
- Es esencial anticiparse a eventos no deseados y diseñar e implantar planes de contingencia efectivos para mantener la actividad de su negocio sin importar qué pueda ocurrir.
- Marco legal en continua evolución.
    - Esquema Nacional de Seguridad
    - Ley de Protección de datos, Habeas Data
    - Cambios en la Unión Europea
    - Leyes y exigencias nuevas para inmigrantes en estados unidos

8.2 QUE HA OCURRIDO RECIENTEMENTE EN LOS ÚLTIMOS AÑOS

8.2.1 FALLAS A NIVEL MUNDIAL

- Averías en cables submarinos afectando a los servicios de Internet de la India,
- Bahrain, Egipto, Emiratos Árabes Unidos y Arabia Saudí.
- Evacuación de más de 2.700 empleados en London Tower Place: vehículo sospechoso en el aparcamiento.
- Huelgas en el transporte público en Francia, España, Alemania, Hungría y Grecia.
- Múltiples eventos - Terremotos, Huelgas, Temporales de Nieve, Explosiones, Cortes intermitentes de suministro eléctrico, Incendios – afectando Atenas (Grecia)
- Fallos de Red/Telefonía afectando Reino Unido, Alemania, Portugal, Italia, España o Suiza
- Aparición del malware llamado Adylkuzz, el cual aprovecha la misma vulnerabilidad explotada por el Ransomware WannaCry (MS17-010 “Eternal Blue”).
- Aparición de un virus de tipo Ransomware denominada Petya, la cual aprovecha la misma vulnerabilidad explotada por el Ransomware WannaCry (MS17-010 “Eternal Blue”)

8.2.2 FALLAS OCURRIDAS EN COLOMBIA Y BARRANQUILLA

- Problemas de desordenes públicos, manifestaciones, huelgas y paros cívicos que afectan la movilidad de los sistemas de Transporte Masivo
- Problemas Eléctricos en las Ciudades de la costa Atlántica por problemas en calidad de servicio o ausencia de suministro eléctrico
- Inundaciones por Lluvias y desbordamientos de Ríos que afectan a ciudades que están alrededor de sus Riveras

La metodología a utilizar en el diseño de un plan de recuperación de desastres, se propone un proceso comprendido desde el inicio del proyecto hasta la realización de las pruebas del DRP, para llevar a cabo esto, se considera el Estándar Australiano / Nueva Zelanda **AS/NZS 4360 para la gestión de riesgos,** del modelo de procesos de **COBIT 5; Proceso DSS04 Gestionar la continuidad**, También la **Norma ISO 22301 – Gestión de la continuidad de Negocio**, con base en lo anterior se diseña una metodología para colocar en funcionamiento un ***Plan de Recuperación de Desastres enfocado en la plataforma informática de Recaudos y de Control de Flota para un sistema de Transporte Masivo de Pasajeros***

La base de la formulación de un **DRP** debe ser entendida como un proceso continuo y de importancia estratégica para la alta Gerencia, se plantea una propuesta con las fases de Planear, Hacer, Verificar y Actuar (PHVA)

Figura No 9: Fases de un ***Plan de Recuperación de Desastres – DRP***
Fuente: Elaboración Propia

8.3 PLANEAR

En esta fase de inicio del proyecto se verifica la empresa, la documentación existente, se define las áreas y personas que intervendrán y que tendrán alguna responsabilidad en el proyecto.

PLANEAR:

- Evaluación de la empresa
- Definir el área o responsable del proyecto de DRP
- Definir áreas y personas que intervendrán en el DRP
- Crear política de Recuperación de Desastres
- Planificación del Proyecto

Figura No 10: ***PLANEAR*** - Fases de un ***Plan de Recuperación de Desastres – DRP***

Fuente: Elaboración Propia

8.3.1 ELABORACIÓN DE LA FASE DE PLANEACIÓN

En esta Fase se presenta la elaboración de la ***PLANEACIÓN***. Se propone analizar la empresa desde los objetivos corporativos.

- Garantizar el cumplimiento y los lineamientos que exige el contrato de concesión entre la empresa concesionaria del Transporte Masivo y el ente gestor.
- Mejora continuamente los servicios de recaudos y de control de flota para aumentar la satisfacción y la confianza de los clientes.
- Garantizar la continuidad de la operación y prestación de los servicios de cara a los clientes externos e internos.
- Satisfacer las necesidades del cliente, empleados para maximizar el valor de cara a las accionistas del negocio.
- Proteger, preservar y administrar objetivamente la información de la empresa frente a amenazas internas o externas bajo un modelo de sistema de gestión de seguridad de la información.

Para el tratamiento de esto comenzamos utilizando el marco de Gobierno de TI – ***COBIT 5*** proceso comprendido para la evaluación de la Empresa utilizando la metodología propuesta de las fases PHVA - ***PLANEAR, HACER, VEIRIFCAR, ACTUAR***

Para el desarrollo de la fase de ***PLANEAR*** se hace un mapeo entre las Metas Corporativas y Objetivos de Corporativos de COBIT 5 y las Metas Relacionadas de TI en COBIT 5

Entre paréntesis se indica a cual corresponde en COBIT 5.0[8]

OBJETIVOS CORPORATIVOS	OBJETIVOS CORPORATIVOS COBIT 5
• Garantizar el cumplimiento y los lineamientos que exige el contrato de concesión entre la empresa concesionaria del Transporte Masivo y el ente gestor. **(4) (15)** • Mejoramiento continuo de los servicios de recaudos y de control de flota para aumentar la satisfacción y la confianza de los clientes **(6)** • Garantizar la continuidad de la operación y prestación de los servicios de cara a los clientes externos e internos **(7)**	**(4)** Cumplimiento de leyes y regulaciones externas (15) Cumplimiento con las políticas internas (6) Cultura de servicio orientada al cliente (7) Continuidad y disponibilidad del servicio de negocio (1) Valor para las partes interesadas de las Inversiones de Negocio **(3)** Riesgos de negocio gestionados (salvaguarda de activo) (8) Respuestas ágiles a un entorno de negocio cambiante

[8] COBIT 5 ***Un Marco de Negocio para el Gobierno y la Gestión de la Empresa" Pagina 50 Fig. 22***

• Satisfacer las necesidades del cliente, empleados para maximizar el valor de cara a las accionistas del negocio **(1)** • Garantizar la disponibilidad y continuidad de los sistemas de información a través de la integración de tecnologías **(8)(7)** • Proteger, preservar y administrar objetivamente la información de la empresa frente a amenazas internas o externas bajo un modelo de sistema de gestión de seguridad de la información **(3)**	

OBJETIVOS CORPORATIVOS COBIT 5	OBJETIVOS DE TI COBIT 5
(4) Cumplimiento de leyes y regulaciones externas	**(02)** Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas (10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones
(15) Cumplimiento con las políticas internas	**(02)** Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas (10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones (15) Cumplimiento de TI con las políticas internas
(6) Cultura de servicio orientada al cliente	(01) Alineamiento de TI y la estrategia de negocio (07) Entrega de servicios de TI de acuerdo a los requisitos del negocio
(7) Continuidad y disponibilidad del servicio de negocio	(04) Riesgos de negocio relacionados con las TI gestionados (10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones (14) Disponibilidad de información útil y relevante para la toma de decisiones
(1) Valor para las partes interesadas de las Inversiones de Negocio	(01) Alineamiento de TI y la estrategia de negocio (03) Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI (05) Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI (07) Entrega de servicios de TI de acuerdo a los requisitos del negocio (11) Optimización de activos, recursos y capacidades de las TI (13) Entrega de Programas que proporción en beneficios a Tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
(8) Respuestas ágiles a un entorno de negocio cambiante	(01) Alineamiento de TI y la estrategia de negocio (07) Entrega de servicios de TI de acuerdo a los requisitos del negocio (09) Agilidad de las TI (17) Conocimiento, experiencia e iniciativas para la innovación de negocio
(3) Riesgos de negocio gestionados (salvaguarda de activo)	(04) Riesgos de negocio relacionados con las TI gestionados (10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones (16) Personal del negocio y de las TI competente y motivado

Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos
(Entre paréntesis se indica a cual corresponde en COBIT 5.0[9]

OBJETIVOS DE TI COBIT 5	PROCESOS COBIT 5
(02) Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	(APO01)Gestionar el Marco de Gestión de TI (APO12) Gestionar el Riesgo (APO13) Gestionar la Seguridad (BAI10) Gestionar la Configuración (DS05) Gestionar los Servicios de Seguridad (MEA02) Supervisar, Evaluar y Valorar el Sistema de Control Interno (MEA03) Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
(10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones	**(**EDM03) Asegurar la Optimización del Riesgo (APO12) Gestionar el Riesgo (APO13) Gestionar la Seguridad (BAI06) Gestionar los Cambios (DS05) Gestionar los Servicios de Seguridad
(15) Cumplimiento de TI con las políticas internas	(EDM03) Asegurar la Optimización del Riesgo (APO01) Gestionar el Marco de Gestión de TI (MEA01) Supervisar, Evaluar y Valorar Rendimiento y conformidad (MEA02) Supervisar, Evaluar y Valorar el Sistema de Control Interno
(01) Alineamiento de TI y la estrategia de negocio	(EDM01) Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno (EDM02) Asegurar la Entrega de Beneficios (APO01) Gestionar el Marco de Gestión de TI (APO02) Gestionar la Estrategia (APO03) Gestionar la Arquitectura Empresarial (APO05) Gestionar el portafolio (APO07) Gestionar los Recursos Humanos (APO08) Gestionar las Relaciones (BAI01) Gestionar los Programas y Proyectos (BAI02) Gestionar la Definición de Requisitos
(07) Entrega de servicios de TI de acuerdo a los requisitos del negocio	(EDM01) Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno (EDM02) Asegurar la Entrega de Beneficios (EDM05) Asegurar la Transparencia hacia las partes interesadas (APO02) Gestionar la Estrategia (APO08) Gestionar las Relaciones (APO09) Gestionar los Acuerdos de Servicio (APO10) Gestionar los Proveedores (APO11) Gestionar la Calidad (BAI02) Gestionar la Definición de Requisitos (BAI03) Gestionar la Identificación y la Construcción de Soluciones (BAI04) Gestionar la Disponibilidad y la Capacidad (BAI06) Gestionar los Cambios (DSS01) Gestionar las Operaciones (DSS02) Gestionar las Peticiones y los Incidentes del Servicio (DSS03) Gestionar los Problemas (DSS04) Gestionar la Continuidad (DSS06) Gestionar los Controles de los Procesos del Negocio (MEA01) Supervisar, Evaluar y Valorar Rendimiento y

[9] COBIT 5.0 "***Un Marco de Negocio para el Gobierno y la Gestión de la Empresa" Pagina 52 Fig. 23***

	Conformidad
(04) Riesgos de negocio relacionados con las TI gestionados	(EDM03) Asegurar la Optimización del Riesgo (APO10) Gestionar los Proveedores (APO12) Gestionar el Riesgo (APO13) Gestionar la Seguridad (BAI01) Gestionar los Programas y Proyectos (BAI06) Gestionar los Cambios (DSS01) Gestionar las Operaciones (DSS02) Gestionar las Peticiones y los Incidentes del Servicio (DSS03) Gestionar los Problemas (DSS04) Gestionar la Continuidad (DSS05) Gestionar los Servicios de Seguridad (DSS06) Gestionar los Controles de los Procesos del Negocio (MEA01) Supervisar, Evaluar y Valorar Rendimiento y Conformidad (MEA02) Supervisar, Evaluar y Valorar el Sistema de Control Interno (MEA03) Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
(14) Disponibilidad de información útil y relevante para la toma de decisiones	(APO09) Gestionar los Acuerdos de Servicio (APO13) Gestionar la Seguridad (BAI04) Gestionar la Disponibilidad y la Capacidad (BAI10) Gestionar la Configuración (DSS03) Gestionar los Problemas (DSS04) Gestionar la Continuidad
(03) Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	(EDM01) Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno (EDM05) Asegurar la Transparencia hacia las partes interesadas
(05) Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	(EDM02) Asegurar la Entrega de Beneficios (APO04) Gestionar la Innovación (APO05) Gestionar el portafolio (APO06) Gestionar el Presupuesto y los Costes (APO11) Gestionar la Calidad (BAI01) Gestionar los Programas y Proyectos
(11) Optimización de activos, recursos y capacidades de las TI	(EDM04) Asegurar la Optimización de los Recursos (APO01) Gestionar el Marco de Gestión de TI (APO03) Gestionar la Arquitectura Empresarial (APO04) Gestionar la Innovación (APO07) Gestionar los Recursos Humanos (BAI04) Gestionar la Disponibilidad y la Capacidad (BAI09) Gestionar los Activos (BAI10) Gestionar la Configuración (DSS01) Gestionar las Operaciones (DSS03) Gestionar los Problemas (MEA01) Supervisar, Evaluar y Valorar Rendimiento y Conformidad
(13) Entrega de Programas que proporción en beneficios a Tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	(APO05) Gestionar el portafolio (APO07) Gestionar los Recursos Humanos (APO11) Gestionar la Calidad (APO12) Gestionar el Riesgo (BAI01) Gestionar los Programas y Proyectos (BAI05) Gestionar la introducción de Cambios Organizativos
(09) Agilidad de las TI	(EDM04) Asegurar la Optimización de los Recursos (APO01) Gestionar el Marco de Gestión de TI (APO03) Gestionar la Arquitectura Empresarial (APO04) Gestionar la Innovación (APO10) Gestionar los Proveedores (BAI08) Gestionar el Conocimiento
(17) Conocimiento, experiencia e iniciativas para la innovación de negocio	(EDM02) Asegurar la Entrega de Beneficios (APO01) Gestionar el Marco de Gestión de TI (APO02) Gestionar la Estrategia

	(APO04) Gestionar la Innovación (APO07) Gestionar los Recursos Humanos (APO08) Gestionar las Relaciones (BAI05) Gestionar la introducción de Cambios Organizativos (BAI08) Gestionar el Conocimiento
(16) Personal del negocio y de las TI competente y motivado	(EDM04) Asegurar la Optimización de los Recursos (APO01) Gestionar el Marco de Gestión de TI (APO07) Gestionar los Recursos Humanos

Se escoge de los Procesos de COBIT 5 el ***(DSS04) Gestionar la Continuidad,*** este proceso lo encontramos alineado con el objetivo corporativo "***Garantizar la continuidad de la operación y prestación de los servicios de cara a los clientes externos e internos"***

DSS04: GESTIONAR LA CONTINUIDAD
Descripción Establecer y mantener un plan que permita a la Empresa y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos de la Compañía y los servicios de TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la Empresa.
Objetivos • Continuar las operaciones críticas de la Compañía y mantener la disponibilidad de la información para la Empresa ante una interrupción significativa.
Indicadores del proceso • Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento. • Porcentaje de restauraciones satisfactorias y a tiempo de copias de seguridad. • Frecuencia de pruebas de continuidad del servicio.
Indicadores de TI • Número de interrupciones del negocio debidas a incidentes en el servicio de TI. • Nivel de satisfacción de los usuarios y disponibilidad de la información de gestión. • Número de incidentes en los procesos de la Compañía causados por la indisponibilidad de la información • Relación de decisiones de la Compañía erróneas causadas por falta de información o por información errónea.
Prácticas clave • Definir la política de continuidad del negocio, objetivos y alcance. • Mantener una estrategia de continuidad. • Desarrollar un plan de continuidad del negocio. • Ejercitar, probar y revisar el plan de continuidad.

- Revisar, mantener y mejorar el plan de continuidad.
- Proporcionar formación en el plan de continuidad.
- Gestionar acuerdos de respaldo.
- Ejecutar revisiones post-reanudación.

Definir la política de continuidad del negocio, objetivos y alcance

Actividades

1. Identificar procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la Empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.
2. Definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad de la Empresa.

Entradas	Salidas
• Acuerdos de nivel de servicio (SLA).	• Política y objetivos de continuidad de negocio.

Mantener una estrategia de continuidad

Actividades

1. Realizar un análisis en la Empresa para evaluar el impacto en tiempo de una interrupción en las funciones críticas de la Compañía y el efecto que tendría en ellas.
2. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.
3. Analizar los requerimientos de continuidad para identificar y seleccionar las posibles estrategias de negocio y opciones técnicas.
4. Obtener la aprobación de la alta dirección para las opciones estratégicas seleccionadas.

Entradas	Salidas
• Comunicaciones del impacto de los riesgos	• Análisis de impacto en el negocio. • Requerimientos de continuidad.

Desarrollar un plan de continuidad del negocio

Actividades

1. Evidenciar que los proveedores clave tengan implantados planes de continuidad efectivos.
2. Definir las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos de la Compañía, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.
3. Definir y documentar los recursos necesarios para soportar los procedimientos de

continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.

Entradas	Salidas
	• Plan de continuidad del negocio (BCP).

Ejercitar, probar y revisar el BCP

Actividades

1. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del BCP para enfrentarse a los riesgos de la Compañía.
2. Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.
3. Realizar un análisis, revisión y recomendaciones post-ejercicio para considerar el logro.

Entradas	Salidas
	• Pruebas de objetivos Interno. • Pruebas de ejercicios Interno. • Pruebas de resultados y recomendaciones.

Revisar, mantener y mejorar el plan de continuidad

Actividades

1. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la Empresa, procesos de negocio, acuerdos de servicio externos, tecnologías, infraestructura, sistemas operativos y aplicaciones.

Entradas	Salidas
	• Resultados de las revisiones de los planes. • Cambios recomendados a los planes.

Proporcionar formación en el plan de continuidad

Actividades

1. Definir y mantener los planes y requerimientos de formación para quienes planifiquen continuamente la continuidad y realicen análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes.
2. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.

Entradas	Salidas
• Lista del personal que requiere formación.	• Requerimientos de formación. • Planes de formación.

Gestionar acuerdos de respaldo

Actividades

1. Asegurar que los sistemas, aplicaciones, datos o documentación estén debidamente respaldados o asegurados en cintas de Backups.

2. Considerar el hecho de contratar una firma especializada en custodiar cintas de Backups	
Entradas	**Salidas** Prueba de los resultados de las copias de seguridad de los datos.
Ejecutar revisiones post-reanudación	
Actividades 1. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, para atender y resolver incidentes de infraestructura técnica. 2. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la Empresa	
Entradas	**Salidas** • Informe de revisión post-reanudación. • Cambios aprobados a los planes.

8.3.2 DEFINICIÓN DE ROLES Y RESPONSABILIDADES

La definición de roles y responsabilidades es uno de los aspectos claves y más importantes del Plan de Recuperación ante desastres, porque aquí se determinan cada una de las actividades de los responsables que ejecutaran el Plan y estas actividades corresponden a las que hay que ejecutar antes, durante y después del desastre, Igualmente, deben establecerse las estructuras organizacionales, los perfiles de los cargos y los procesos, que darán sostenibilidad a la continuidad del servicio de TI

Para que un plan de recuperación ante desastres funcione, se debe involucrar a la gerencia. Ellos son los responsables de su coordinación y deben asegurar su efectividad. Adicionalmente, deben proveer los recursos necesarios para un desarrollo efectivo del plan. Todos los departamentos de la organización participan en la definición del plan

Para la definición de los roles de responsabilidades de la fase de ***PLANEAR*** se hace con una Matriz RACI[10] en base a los resultados que nos arrojo el Mapeo de Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI se escoge el "**PROCESO COBIT 5 – DSS04 Gestionar la Continuidad** " y "**BAI06 Gestionar los Cambios"**

[10] **Matriz RACI:** Corresponde a la matriz de la asignación de responsabilidades, RACI por las iniciales de los tipos de responsabilidad R: Responsible: Encargado; A: Accountable, Responsable; C: Consulted, Consultado; I: Informed, Informado

Procesos COBIT 5 escogidos para elaborar la Matriz de responsabilidades RACI[11]

(Anexo 3)

OBJETIVOS DE TI COBIT 5 - (04) Riesgos de negocio relacionados con las TI gestionados

PROCESOS COBIT 5 – (DSS04) Gestionar la Continuidad

OBJETIVOS DE TI COBIT 5 - (14) Disponibilidad de información útil y relevante para la toma de decisiones

PROCESOS COBIT 5 – (DSS04) Gestionar la Continuidad

MATRIZ RACI

OBJETIVOS DE TI COBIT 5 - (04) Riesgos de negocio relacionados con las TI gestionados

OBJETIVOS DE TI COBIT 5 - (14) Disponibilidad de información útil y relevante para la toma de decisiones

PROCESOS COBIT 5 – (DSS04) Gestionar la Continuidad

R	Encargado
A	Responsable
C	Consultado
I	Informado

PROCESO - APO03	Junta Directiva	Gerente General - CEO	Gerente Financiero - CFO	Gerencia Tecnica/Operativa - COO	Director de Recaudos	Propietarios de los Procesos de Ne	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Pro	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Inform	Consejo de Arquitectura de la Emp	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Cumplia	Auditoría	Director de Gestión e Información	Director de Mantenimiento	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manage	Gestor de Seguridad de la Informac	Gestor de Continuidad de Negocio	Gestor de Privacidad de la informa
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Mantener una estrategia de continuidad.				A	C	R					I					C	C	R	R	C	R					R	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.					I	R									I	C	C	R	C	C	R					A	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad					I	R									I		R	R		C	R					A	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.				A	I	R					I							R		C	R					R	
DSS04.06 Proporcionar formación en el plan de continuidad					I	R												R		R	R	R				A	
DSS04.07 Gestionar acuerdos derespaldo.																				C	A					R	
DSS04.08 Ejecutar revisiones postreanudación					C	R					I							R	C	C	R	R				A	

[11] **RACI: COBIT 5.0 "*Procesos Catalizadores*" *Matriz RACI DSS004 - Gestionar la Continuidad - Página 186***

Procesos COBIT 5 escogidos para elaborar la Matriz de responsabilidades RACI[12] (Anexo 3)

OBJETIVOS DE TI COBIT 5 - (10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones
PROCESOS COBIT 5 - (BAI06) Gestionar los Cambios

MATRIZ RACI

OBJETIVOS DE TI COBIT 5 - (10) Seguridad de la información, infraestructuras de procesamiento y aplicaciones

PROCESOS COBIT 5 - (BAI06) Gestionar los Cambios

R	Encargado
A	Responsable
C	Consultado
I	Informado

PROCESO - BAI06	Junta Directiva	**Gerente General - CEO**	**Gerente Financiero - CFO**	**Gerencia Tecnica/Operativa - COO**	**Director de Recaudos**	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	**Director de Gestión e Información (CIO)**	**Director de Mantenimiento**	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Gestionar cambios de emergencia					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Hacer seguimiento e informar de cambios de estado.					C	R			C									A		R	R		R			
BAI06.04 Cerrar y documentar los cambios					A	R			R		C					C	C	R	C	R	R	I	I			

[12] **RACI: COBIT 5.0 "*Procesos Catalizadores*" *Matriz RACI BAI06 - Gestionar los Cambios - Página 149***

8.3.3 POLITICA DE RECUPERACIÓN DE DESASTRES

El **DRP** ***"Plan de Recuperación de Desastres"*** diseñado para la empresa concesionaria de la operación y explotación del sistema Integrado de Transporte masivo de pasajeros del Distrito de Barranquilla, tiene como fin el de mantener la disponibilidad de la plataforma tecnológica del sistema de Recaudos y de Control de Flota, de acuerdo a los lineamientos exigidos en el contrato de concesión.

Dado las condiciones del sistema de Transporte masivo de pasajeros y debido a las exigencias contractuales de mantener un nivel de disponibilidad del 98,6% y solucionar los inconvenientes en un tiempo menor a 90 minutos, el **DRP** tendrá como objetivo ayudar a restablecer el servicio en un tiempo menor o igual al máximo permitido, durante la operación diaria.

8.3.4 OBJETIVOS DEL DRP

Garantizar que la plataforma tecnológica del sistema recaudos y de control de flota del transporte masivo de pasajeros esté disponible en un 98,6 %, durante su operación, en caso de presentarse un incidente o afectación de la operación del sistema, este deberá solucionar los inconvenientes presentados en un tiempo menor a 90 minutos

Establecer las precauciones que se deberán aplicar para que los efectos de un desastre se reduzcan al mínimo y la empresa sea capaz de mantener o reanudar rápidamente las funciones de sus sistemas de misión crítica.

8.3.5 PLANIFICACIÓN DEL DRP

La Gerencia Técnico operativo de la empresa concesionaria será responsable del desarrollo del **DRP** ***"Plan de Recuperación de Desastres"***, planeando, y definiendo todas las políticas que se deben llevar a cabo, la Dirección de Gestión e Información (CIO) junto con su equipo de colaboradores serán los encargados de tomar las acciones que deben llevarse a cabo durante un evento de contingencia y de que todas las actividades se cumplan de acuerdo a lo planeado

8.4 HACER

HACER:

- Analisis de Impacto de Negocio - BIA
- Evaluación y Gestión del Riesgo
- Controles Existentes
- Controles Recomendados
- Matriz de Riesgos
- Mapa de Riesgos
- Estrategias de Recuperación
- Procedimientos de Recuperación
- Capacitación

Figura No 11: ***HACER*** - Fases de un ***Plan de Recuperación de Desastres – DRP***
Fuente: Elaboración Propia

8.4.1 ANALISIS DE IMPACTO

En un plan de Recuperación de desastres el análisis de impacto sobre el negocio es uno de los aspectos más importantes a considerar, se trata de identificar los diversos eventos que pudiesen afectar la continuidad de los sistemas de información críticos, para el caso de estudio será el análisis de impacto sobre la plataforma de control de flota y de recaudos de un sistema de Transporte masivo de pasajeros teniendo en cuenta los siguientes aspectos:

1) Identificar sitios físicos: Se valida la lista de instalaciones físicas, áreas o entidades en donde opera los servicio de TI de la empresa.
2) Identificar sistemas de información: Se obtiene la lista de los sistemas de información que se poseen en cada instalación y se determina cuáles de ellos están relacionados de manera directa o indirecta con el servicio de TI.
3) Evaluar la criticidad de los sistemas de información: Se califica la criticidad de cada uno de los procesos relacionados con la Empresa, haciendo uso de la tabla de criticidad previamente definida
4) Determinar el tiempo de recuperación de cada sistema: Se estima el tiempo de recuperación objetivo, el punto de recuperación objetivo y el tiempo máximo tolerable fuera de servicio para cada proceso

8.4.2 EVALUACIÓN Y GESTIÓN DEL RIESGO

La gestión de riesgo es el punto central de una estrategia de seguridad esta debe estar perfectamente alineada con la visión de la empresa, dentro de su entorno de operación para lo cual se utilizan las mejores prácticas que recomienda ITIL para la gestión de servicios de T.I. y las metodologías recibidas en clase de la Maestría de Gobierno de T.I. para la evaluación y tratamiento del riesgo, basadas en el estándar Australiano ***AS / NZS 4360 para la Gestión de Riesgos***

IDENTIFICAR AMENAZAS SOBRE LOS SISTEMAS

La empresa debe preparar un análisis de riesgo y crear una lista de posibles desastres naturales o causados por errores humanos y clasificarlos según sus probabilidades. Una vez terminada la lista, cada departamento debe analizar las posibles consecuencias y el impacto relacionado con cada tipo de desastre.

Esto servirá como referencia para identificar lo que se necesita incluir en el plan. Un plan completo debe considerar una pérdida total del centro de datos y eventos de larga duración de más de una semana. Una vez definidas

las necesidades de cada departamento, se les asigna una prioridad. Los procesos y operaciones son analizados para determinar la máxima cantidad de tiempo que la organización puede sobrevivir. Posteriormente, debe establecerse un orden de recuperación según el grado de importancia.

IDENTIFICAR VULNERABILIDADES
Una de las preocupaciones más importantes que atañe a la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de los Hackers que con herramientas de software y conocimientos avanzados las usan para ocasionar daños a los sistemas de información

PROBABILIDAD DE OCURRENCIA DEL EVENTO
La probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de energía eléctrica, falla en las comunicaciones, u otros eventos, se podrían sacar de estadísticas vividas por la empresa y publicaciones de firmas especializadas de publicaciones tecnológicas como, info security news magazine.

8.4.2.1 METODOLOGÍA UTILIZADA PARA EL ANÁLISIS DE RIESGOS

8.4.2.1.1 *Listar las posibles causas de riesgos de desastre para la plataforma informática de recaudos y control de flota*.

Los incidentes a tener en cuenta y que se trabajaran en el Plan de Recuperación de Desastres son, riesgos asociados a:

1) Problemas eléctricos,
2) Incendios por cortos eléctricos
3) Problemas con UPS de estación
4) Problemas con Planta Eléctrica de Estación
5) Desastre Natural: (Aguas Lluvias, Inundación, Terremoto)
6) Problemas con Aires Acondicionados (Condensación de AA)
7) Recalentamiento en Data Center o Estaciones
8) Problemas por Cortes de Fibra óptica
9) Problemas por Falta de Servicio de Internet
10) Problemas de desorden público
11) Errores humanos
12) Problemas con equipos de comunicaciones
13) Problemas con servidores
14) Problemas con Storage de Discos Duros

15) Problemas con el no cumplimiento de los niveles de servicio contractuales
16) Problemas por no prestación de servicios de Venta y Recarga de pasajes
17) Problemas por la compra constante de repuestos para reparar dispositivos por fallas eléctricas

8.4.2.1.2 *Seleccionar de los siguientes impactos, los que más aplican para el proyecto*

Los Impactos a tener en cuenta y que se trabajaran en el Plan de Recuperación de Desastres son, impactos asociados a:

1) Impacto en la continuidad del servicio por Problemas eléctricos,
2) Impacto en la continuidad del servicio por Incendios por cortos eléctricos
3) Impacto en la continuidad del servicio por Problemas con UPS de estación
4) Impacto en la continuidad del servicio por Problemas con Planta Eléctrica de Estación
5) Impacto en la continuidad del servicio por Desastre Natural: (Aguas Lluvias, Inundación, Terremoto)
6) Impacto en la continuidad del servicio por Problemas con Aires Acondicionados (Condensación de AA)
7) Impacto en la continuidad del servicio por Recalentamiento en Data Center o Estaciones
8) Impacto en la continuidad del servicio por Problemas por Cortes de Fibra óptica
9) Impacto en la continuidad del servicio por Problemas por Falta de Servicio de Internet
10) Impacto en la continuidad del servicio por Problemas de desorden público
11) Impacto en la continuidad del servicio por Errores humanos
12) Impacto en la continuidad del servicio por Problemas con equipos de comunicaciones
13) Impacto en la continuidad del servicio por Problemas con servidores
14) Impacto en la continuidad del servicio por Problemas con Storage de Discos Duros
15) Impacto en la continuidad del servicio por Problemas con el no cumplimiento de los niveles de servicio contractuales

16) Impacto Financiero debido a la no prestación de servicios de Venta y Recarga de pasajes
17) Impacto Financiero debido a la compra constante de repuestos para reparar dispositivos por fallas eléctricas

8.4.2.1.3 *Con los impactos seleccionados en el punto anterior, redactamos los riesgos en términos de "impacto debido a".*

#	RIESGOS
R1	Impacto en la continuidad del servicio por Problemas eléctricos,
R2	Impacto en la continuidad del servicio por Incendios por cortos eléctricos
R3	Impacto en la continuidad del servicio por Problemas con UPS de estación
R4	Impacto en la continuidad del servicio por Problemas con Planta Eléctrica de Estación
R5	Impacto en la continuidad del servicio por Desastre Natural: (Aguas Lluvias, Inundación, Terremoto)
R6	Impacto en la continuidad del servicio por Problemas con Aires Acondicionados (Condensación de AA)
R7	Impacto en la continuidad del servicio por Recalentamiento en Data Center o Estaciones
R8	Impacto en la continuidad del servicio por Problemas por Cortes de Fibra óptica
R9	Impacto en la continuidad del servicio por Problemas por Falta de Servicio de Internet
R10	Impacto en la continuidad del servicio por Problemas de desorden público
R11	Impacto en la continuidad del servicio por Errores humanos
R12	Impacto en la continuidad del servicio por Problemas con equipos de comunicaciones
R13	Impacto en la continuidad del servicio por Problemas con servidores
R14	Impacto en la continuidad del servicio por Problemas con Storage de Discos Duros
R15	Impacto Financiero por multas con el no cumplimiento de los niveles de servicio contractuales
R16	Impacto Financiero debido a la no prestación de servicios de Venta y Recarga de pasajes
R17	Impacto Financiero debido a la compra constante de repuestos para reparar dispositivos por fallas eléctricas

8.4.2.1.4 *Identificar los controles existentes (si los hay), para los riegos del punto anterior.*

#	RIESGOS	CONTROLES EXISTENTES
R1	Impacto en la continuidad del servicio por Problemas eléctricos,	Protecciones eléctricas con UPS y Plantas Eléctricas
R2	Impacto en la continuidad del servicio por Incendios por cortos eléctricos	Póliza de Seguros
R3	Impacto en la continuidad del servicio por Problemas con UPS de estación	Contratos de Mantenimiento a UPS
R4	Impacto en la continuidad del servicio por Problemas con Planta Eléctrica de Estación	Contrato de Mantenimiento a Plantas Eléctricas
R5	Impacto en la continuidad del servicio por Desastre Natural: (Aguas Lluvias, Inundación, Terremoto)	Póliza de Seguros
R6	Impacto en la continuidad del servicio por Problemas con Aires Acondicionados (Condensación de AA)	Contrato de Mantenimiento a Aires Acondicionados de Precisión Capacitación en Mantenimiento y reparación de Aires acondicionados a personal de Mantenimiento
R7	Impacto en la continuidad del servicio por Recalentamiento en Data Center o Estaciones	Capacitación en Mantenimiento y reparación de Aires acondicionados a personal de Mantenimiento
R8	Impacto en la continuidad del servicio por Problemas por Cortes de Fibra óptica	Contrato de Soporte, Mantenimiento y Reparación de Fibra óptica
R9	Impacto en la continuidad del servicio por Problemas por Falta de Servicio de Internet	Internet por Fibra óptica Internet de contingencia por ADSL
R10	Impacto en la continuidad del servicio por Problemas de desorden público	Póliza de Seguros
R11	Impacto en la continuidad del servicio por Errores humanos	
R12	Impacto en la continuidad del servicio por Problemas con equipos de comunicaciones	Contrato de Soporte Técnico con empresa especialista en comunicaciones
R13	Impacto en la continuidad del servicio por Problemas con servidores	Stock de Repuestos Personal del área de T.I. Entrenado
R14	Impacto en la continuidad del servicio por Problemas con Storage de Discos Duros	Stock de Repuestos Personal del área de T.I. Entrenado
R15	Impacto Financiero por multas con el no cumplimiento de los niveles de servicio contractuales	Personal Entrenado para cumplir con los niveles de servicio contractuales
R16	Impacto Financiero debido a la no prestación de servicios de Venta y Recarga de pasajes	Personal Entrenado para cumplir con los niveles de servicio contractuales
R17	Impacto Financiero debido a la compra constante de repuestos para reparar dispositivos por fallas eléctricas	

8.4.2.1.5 *Recomendar nuevos controles para tratar los riesgos identificados*.

#	RIESGOS	CONTROLES RECOMENDADOS
R1	Impacto en la continuidad del servicio por Problemas eléctricos,	Protecciones eléctricas adicionales de sobre voltajes y supresores de picos para proteger UPS
R2	Impacto en la continuidad del servicio por Incendios por cortos eléctricos	Póliza de Seguros
R3	Impacto en la continuidad del servicio por Problemas con UPS de estación	Contratos de Mantenimiento a UPS, exigir mejorar los acuerdos operativos UPS de Contingencia en Stock
R4	Impacto en la continuidad del servicio por Problemas con Planta Eléctrica de Estación	Contrato de Mantenimiento a Plantas Eléctricas. Plantas eléctricas adicionales en Stock
R5	Impacto en la continuidad del servicio por Desastre Natural: (Aguas Lluvias, Inundación, Terremoto)	Contratar impermeabilización y Reparaciones de los techos en estaciones
R6	Impacto en la continuidad del servicio por Problemas con Aires Acondicionados (Condensación de AA)	Implementar Herramientas de des humificación para cuartos de datos en estaciones
R7	Impacto en la continuidad del servicio por Recalentamiento en Data Center o Estaciones	Instalar Aire Acondicionado de Precisión de contingencia en Data Centers
R8	Impacto en la continuidad del servicio por Problemas por Cortes de Fibra óptica	Mejorar la seguridad en los registros de los ductos por donde pasa la fibra óptica
R9	Impacto en la continuidad del servicio por Problemas por Falta de Servicio de Internet	Contratar un proveedor de servicios de internet adicional, para contingencia debido a que los servicios Internet actuales esta con un solo proveedor
R10	Impacto en la continuidad del servicio por Problemas de desorden público	Póliza de Seguros
R11	Impacto en la continuidad del servicio por Errores humanos	Incluir una póliza de seguros contra terceros que cubra este tipo de errores
R12	Impacto en la continuidad del servicio por Problemas con equipos de comunicaciones	Tener equipos de comunicaciones y partes de estos en stock
R13	Impacto en la continuidad del servicio por Problemas con servidores	Stock de Servidores para Control de Flota y Recaudos del modelo de producción
R14	Impacto en la continuidad del servicio por Problemas con Storage de Discos Duros	Solicitar Extensión de Garantía adicional con el fabricante

R15	Impacto Financiero por multas con el no cumplimiento de los niveles de servicio contractuales	Programar entrenamientos adicionales para mejorar al personal existente y programar al nuevo personal
R16	Impacto Financiero debido a la no prestación de servicios de Venta y Recarga de pasajes	Programar entrenamientos adicionales para mejorar al personal existente y programar al nuevo personal
R17	Impacto Financiero debido a la compra constante de repuestos para reparar dispositivos por fallas eléctricas	Tener un Stock Base de repuestos de las partes de los dispositivo que más sufren averías

8.4.2.2 PRIORIZACIÓN DE RIESGOS:

Cálculo de Valor de Activos

VALORACIÓN DE ACTIVOS	
ACTIVO	**VALOR**
▪ Edificio	$1.000 millones
▪ Ups ▪ Aires Acondicionados ▪ Servidores ▪ Dispositivos de Recaudos	$ 80. Millones $ 80. Millones $ 4.500 Millones $ 3.500 Millones
TOTAL	$ 9.160 MILLONES

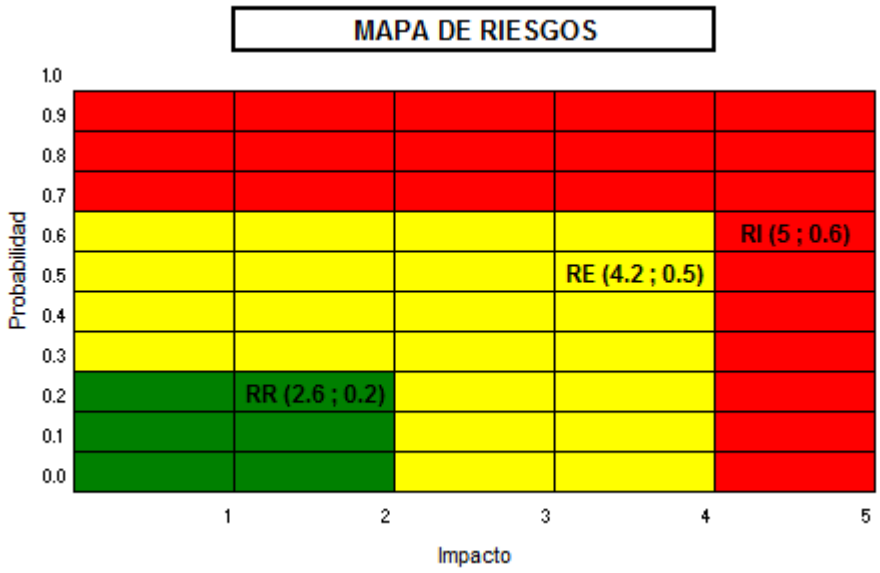
PÉRDIDA FINANCIERA	
Valor	**Descripción**
5	$8001 - $12.000 millones
4	$3001 - $8000 millones
3	$1001 - $3000 millones
2	$501 - $1000 millones
1	0 - $500 millones

8.4.2.3 MATRIZ DE RIESGOS (Anexo 2)

PLATAFORMA INFORMÁTICA DE RECAUDOS Y CONTROL DE FLOTA DE UN SISTEMA DE TRANSPORTE MASIVO DE PASAJEROS
MATRIZ DE RIESGOS

#	RIESGO	RIESGO INHERENTE		CONTROLES EXISTENTES	RIESGO DE EXPOSICIÓN		CONTROLES RECOMENDADOS	RIESGO RESIDUAL	
		IMPACTO	PROBABILIDAD		IMPACTO	PROBABILIDAD		IMPACTO	PROBABILIDAD
R1	Impacto en la continuidad del servicio por Problemas eléctricos,	5	0,9	Protecciones eléctricas con UPS y Plantas Eléctricas	5	0,9	Protecciones eléctricas adicionales de sobre voltajes y supresores de picos para	3	0,2
R2	Impacto en la continuidad del servicio por Incendios por cortos eléctricos	5	0,1	Póliza de Seguros	5	0,1	Póliza de Seguros	5	0,1
R3	Impacto en la continuidad del servicio por Problemas con UPS de estación	5	0,5	Contratos de Mantenimiento a UPS	3	0,3	Contratos de Mantenimiento a UPS, exigir mejorar los acuerdos operativos UPS de Contingencia en Stock	3	0,2
R4	Impacto en la continuidad del servicio por Problemas con Planta Eléctrica de Estación	5	0,5	Contrato de Mantenimiento a Plantas Eléctricas	5	0,1	Contrato de Mantenimiento a Plantas Eléctricas. Plantas eléctricas adicionales en Stock	3	0,1
R5	Impacto en la continuidad del servicio por Desastre Natural: (Aguas Lluvias, Inundación, Terremoto)	5	0,8	Póliza de Seguros	5	0,5	Contratar impermeabilización y Reparaciones de los techos en estaciones	3	0,2
R6	Impacto en la continuidad del servicio por Problemas con Aires Acondicionados (Condensación de AA)	5	0,8	Contrato de Mantenimiento a Aires Acondicionados de Precisión Capacitación en Mantenimiento y reparación de Aires acondicionados a personal de Mantenimiento	4	0,5	Implementar Herramientas de des humificación para cuartos de datos en estaciones	3	0,3
R7	Impacto en la continuidad del servicio por Recalentamiento en Data Center o Estaciones	5	0,5	Capacitación en Mantenimiento y reparación de Aires acondicionados a personal de Mantenimiento	3	0,3	Instalar Aire Acondicionado de Precisión de contingencia en Data Centers	2	0,1
R8	Impacto en la continuidad del servicio por Problemas por Cortes de Fibra óptica	5	0,9	Contrato de Soporte, Mantenimiento y Reparación de Fibra óptica	5	0,5	Mejorar la seguridad en los registros de los ductos por donde pasa la fibra optica	4	0,1
R9	Impacto en la continuidad del servicio por Problemas por Falta de Servicio de Internet	5	0,3	Internet por Fibra óptica Internet de contingencia por ADSL	4	0,5	Contratar un proveedor de servicios de internet adicional, para contingencia debido a que los servicios Internet actuales esta con un solo proveedor	2	0,1
R10	Impacto en la continuidad del servicio por Problemas de desorden público	5	1,0	Póliza de Seguros	5	1,0	Póliza de Seguros	3	0,8
R11	Impacto en la continuidad del servicio por Errores humanos	5	0,2		4	0,2	Incluir una póliza de seguros contra terceros que cubra este tipo de errores	2	0,1
R12	Impacto en la continuidad del servicio por Problemas con equipos de comunicaciones	5	0,5	Contrato de Soporte Técnico con empresa especialista en comunicaciones	4	0,5	Tener equipos de comunicaciones y partes de estos en stock	1	0,1
R13	Impacto en la continuidad del servicio por Problemas con servidores	5	0,5	Stock de Repuestos Personal del área de T.I. Entrenado	5	0,5	Stock de Servidores para Control de Flota y Recaudos del modelo de producción	3	0,3
R14	Impacto en la continuidad del servicio por Problemas con Storage de Discos Duros	5	0,8	Stock de Repuestos Personal del área de T.I. Entrenado	4	0,8	Solicitar Extensión de Garantía adicional con el fabricante	2	0,4
R15	Impacto Financiero por multas con el no cumplimiento de los niveles de servicio contractuales	5	0,5	Personal Entrenado para cumplir con los niveles de servicio contractuales	5	0,5	Programar entrenamientos adicionales para mejorar al personal existente y programar al nuevo personal	3	0,3
R16	Impacto Financiero debido a la no prestación de servicios de Venta y Recarga de pasajes	5	0,3	Personal Entrenado para cumplir con los niveles de servicio	3	0,2	Programar entrenamientos adicionales para mejorar al personal existente y	2	0,1
R17	Impacto Financiero debido a la compra constante de repuestos para reparar dispositivos por fallas eléctricas	5	0,8		3	0,5	Tener un Stock Base de repuestos de las partes de los dispositivo que más sufren averias	1	0,1
	PROMEDIO	5	0,6		4,2	0,5		2,6	0,2
	TOTAL	2,9			2			0,6	

8.4.2.4 MAPA DE RIESGOS (Anexo 2)



8.4.3 ESTRATEGIAS DE RECUPERACIÓN

En esta etapa se determina las mejores alternativas para proceder en caso de un desastre. Todos los aspectos de la organización son analizados, incluyendo hardware, software, comunicaciones, archivos, bases de datos, instalaciones, etc. Las alternativas a considerar varían según la función del equipo y pueden incluir duplicación de centros de datos, alquiler de equipos e instalaciones, contratos de almacenamiento y muchas más. Igualmente, se analiza los costos asociados.

COMPONENTES ESENCIALES

Entre los datos y documentos que se deben proteger están las copias de seguridad de Información, de software y cualquier otra lista importante de elementos de cómputo a considerar podrían ser:

Sistemas telefónicos

- Redes Locales
- Redes WAN
- Redes MAN
- Internet
- Personas
- Infraestructura física
- Aplicaciones
- Hardware
- Bases de datos
- Sistemas operativos
- Firewalls
- Proxy

- IDS
- Switchs de comunicaciones
- Routers

8.4.4 CAPACITACIÓN

En esta etapa se brinda al personal que interactúa con el **DRP** las capacitaciones acordes a las acciones que se deben seguir para permitir una optima utilización del plan de Recuperación de Desastres, se determina las mejores alternativas de capacitación para que quienes interactúan puedan proceder en caso de un siniestro o desastre que afecte la operación, el hardware, software, comunicaciones, archivos, bases de datos, instalaciones, etc.

8.5 VERIFICAR

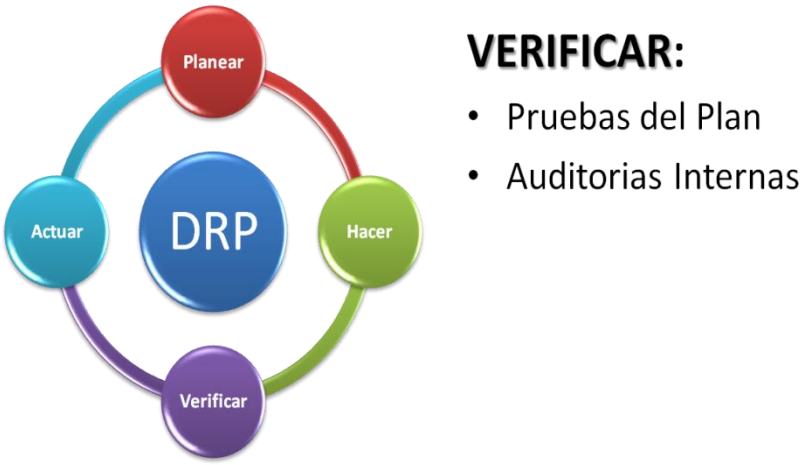


Figura No 12: ***VERIFICAR*** - Fases de un ***Plan de Recuperación de Desastres – DRP***
Fuente: Elaboración Propia

8.5.1 PRUEBAS DEL PLAN

Los planes de recuperación deben ser probados en su totalidad por lo menos una vez al año. La documentación debe especificar los procedimientos y la frecuencia con que se realizan las pruebas. Las razones principales para probar el plan son: verificar la validez y funcionalidad del plan, determinar la compatibilidad de los procedimientos e instalaciones, identificar áreas que necesiten cambios, entrenar a los empleados y demostrar la habilidad de la organización de recuperarse de un desastre. Después de las pruebas el plan debe ser actualizado. Se sugiere que la prueba original se realice en horas que

minimicen trastornos en las operaciones. Una vez demostrada la funcionalidad del plan, se debe hacer pruebas adicionales donde todos los empleados tengan acceso virtual y remoto a estas posiciones y funciones en el caso de un desastre.

Es bien importante que las pruebas se lleven a cabo por las personas que serían responsables de las actividades en una crisis.

Estas pruebas deben tener lo siguiente:

- Desarrollo de los objetivos y alcance de la prueba
- Configuración del ambiente de prueba
- Preparación de los datos de la prueba
- Identificación de quién dirigirá la prueba
- Identificación de quién controla y supervisa la prueba
- Preparación de cuestionarios de evaluación
- Preparación de presupuesto para la fase de prueba
- Entrenamiento a los grupos de prueba de las unidades de negocio

8.6 ACTUAR

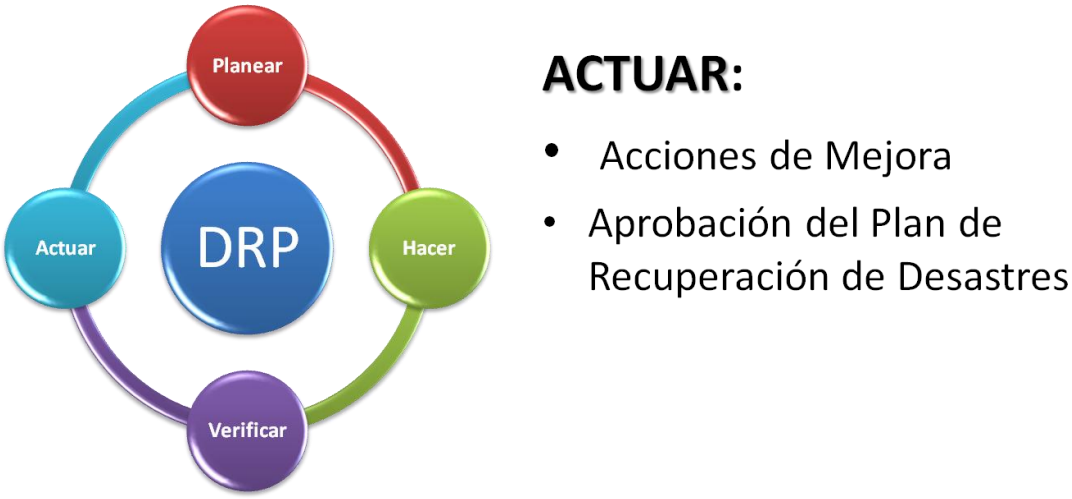


Figura No 13: *ACTUAR* - Fases de un *Plan de Recuperación de Desastres – DRP*
Fuente: Elaboración Propia

8.6.1 ACCIONES DE MEJORA

El plan de Recuperación de Desastres deberá ser sometido a un ciclo de mejora continua, ya que algunos factores pueden afectar su funcionamiento debido a:

- Cambio de personal
- Actualizaciones a nivel de infraestructura tecnológica
- Adquisición o Desarrollo de nuevas aplicaciones
- Cambios en la estrategia de Negocio de la organización

8.6.2 APROBACION FINAL

Después de que el plan haya sido puesto a prueba y corregido, la gerencia deberá aprobarlo. Ellos son los encargados de establecer las pólizas, los procedimientos y responsabilidades en caso de contingencia, de actualizar y dar el visto al plan anualmente. También se recomienda evaluar los planes de contingencia de proveedores externos. El plan de recuperación ante desastres debe ser considerado un seguro fundamental. A pesar de que requiere una cantidad considerable de recursos y dedicación, es una herramienta vital para la supervivencia de las organizaciones.

8.7 DISEÑO RESUMEN DE LAS FASES PARA ELABORAR UN DRP

Figura No 14: *DISEÑO* - Fases de un *Plan de Recuperación de Desastres – DRP*
Fuente: Elaboración Propia

9. ELABORACIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES

La metodología a utilizar en la elaboración de un **DRP "***Plan de recuperación de desastres*" debe ser entendida como un proceso continuo y de importancia estratégica para la alta Gerencia, se plantea una propuesta de las fases ***PLANEAR, HACER, VERIFICAR Y ACTUAR*** (PHVA) con base a la **Norma ISO 22301 – Gestión de la continuidad de Negocio**

A cada una de estas Fases del ciclo PHVA Se Aplican las siguientes normas estándares:

- **Planear**: *COBIT 5; Proceso DSS04* ***- Gestionar la continuidad***
- **Hacer:** *Estándar Australiano / Nueva Zelanda AS/NZS 4360-* ***Gestión de Riesgos***
- **Verificar:** ***ITIL,*** *Biblioteca de Infraestructura de Tecnologías de Información* - **Diseño del servicio**
- **Actuar:** ***ITIL,*** ***-*** *Biblioteca de Infraestructura de Tecnologías de Información* ***– Mejora Continua***

9.1 PLAN DE RECUPERACIÓN DE DESASTRES PROPUESTO

9.1.1 ESCENARIOS: Fallas Ocurridas en Colombia – Barranquilla, Sistema de Transporte Masivo

Problemas Eléctricos en las Ciudades de la costa Atlántica debido a problemas en calidad de servicio o ausencia de suministro eléctrico.

9.1.1.1 PROCEDIMIENTOS - Problemas Eléctricos

PLANEAR	Elementos que debemos tener en cuenta para minimizar el riesgo
HACER	Acciones a Ejecutar
VERIFICAR	Las mediciones con las que probamos que funciona el PLAN
ACTUAR	Procedimientos a seguir

9.1.1.2 Tratamiento a Falla en energía eléctrica para Estaciones

PLANEAR	UPS de 6 KVA, Baterías Adicionales con autonomía superior a 4 Horas; Software de Monitoreo de UPS, Planta Eléctrica, Dispositivos de contingencia para estaciones, Validadores, PDAS,
HACER	Instalación de UPS, con sus Baterías Adicionales, Planta Eléctrica, Configuraciones de RED de la UPS, Registro de la UPS en el software de Monitoreo
VERIFICAR	Se verifican voltajes apropiados y que UPS ha sido detectada por el software de Monitoreo, Personal del CAT, capacitado para coordinar las acciones a seguir con el personal Técnico de Zona
ACTUAR	Procedimientos para garantizar la continuidad del servicio de recaudos y de control de flota, gracias al suministro eléctrico

	de contingencia suministrado a través de la Planta eléctrica y UPS a los dispositivos de la estación

9.1.1.3 Solución a Falla en energía eléctrica para Estaciones:

La Empresa Concesionaria, instalo para cada Estación una UPS de 6 KVA con Banco de Baterías Adicional la cual da una Autonomía superior a 4 Horas, a su vez se encuentra implementado un software que monitorea el Estado de las UPS y Genera una Alerta al CAT en Caso de Falla o Caída de la energía eléctrica en la Estación. Adicional a las UPS se cuenta con 8 plantas eléctricas las cuales pueden ser transportadas y conectadas a las estaciones para garantizar el suministro eléctrico cuando los cortes se extiendan un tiempo mayor al que puedan soportar las UPS. En caso de que la falla se extienda a un número mayor de estaciones, también se cuenta con validadores portátiles y PDAs los cuales garantizar la atención en las estaciones, inclusive si no se encuentra suministro eléctrico de ningún tipo.

- Este Tipo de Incidencias Genera una Llamada de Servicio la cual se asigna al Técnico de la Zona
- El Técnico de la Zona se Desplaza a la Estación constata que los Periféricos de la Estación se encuentran en Servicio
- El Técnico de soporte de Mantenimiento en la empresa monitorea el Estado de la UPS con el software de Gestión con el porcentaje de Autonomía de la UPS y el Tiempo estimado que puede soportar las baterías
- Una Vez el Nivel de Carga de energía de la UPS llega al 70% de autonomía Genera la orden de servicio para que envíen la Planta eléctrica a la Estación que se encuentra Sin energía, dando Tiempo a que llegue la Planta a la Estación se Conecte y esta suministre la Energía necesaria hasta que nuevamente retorne la energía eléctrica a la Estación.
- Cuando se Normaliza la energía se desconecta la Planta se deja la estación en operación normal con el fluido eléctrico de la Estación, se regresa la planta eléctrica a la Empresa, se documenta la Llamada de Servicio y se Cierra el caso.

9.1.1.4 Tratamiento a Falla en energía eléctrica en Data Center

PLANEAR	UPS de 20 KVA, Baterías Adicionales con autonomía superior a 4 Horas; Software de Monitoreo de UPS, Planta Eléctrica de 156 KVA las cuales dan autonomía a los Servidores del data Center y a los computadores de las diversas áreas de
HACER	Instalación de UPS, con sus Baterías Adicionales, Planta Eléctrica, Configuraciones de RED de la UPS, Registro de la UPS en el software de Monitoreo

VERIFICAR	Se verifican voltajes apropiados y que UPS ha sido detectada por el software de Monitoreo, Personal del CAT, capacitado para coordinar las acciones a seguir con el personal Técnico de Zona
ACTUAR	Procedimientos para garantizar la continuidad del servicio de recaudos y de control de flota, gracias al suministro eléctrico de contingencia suministrado a través de la Planta eléctrica y UPS a los dispositivos de la estación

9.1.1.5 Solución Falla en energía eléctrica para Data Center:

En las Instalaciones de RSIT se cuenta con planta eléctrica Trifásica de 156 KVA de conmutación automática la cual cubre la totalidad de la sede en caso de Presentarse la caída eléctrica a las Instalaciones de RSIT y adicional a esto Para el Data Center se cuenta con dos UPS de 20 KVA las cuales dan autonomía a los Servidores del data Center y a los computadores de las diversas áreas de RSIT.

- Para Este Tipo de Incidencias Genera una Llamada de Servicio desde el CAT al analista de soporte del área
- El Analista del área revisa el software de monitoreo de UPS y constata que la autonomía de las Baterías estén en optimo Respaldo
- Segundos después de la caída la energía eléctrica debe Iniciar la Planta eléctrica
- Se debe estar monitoreando la cantidad de ACPM que Requiere la Planta eléctrica para determinar con el paso de las horas si es necesario recargar el combustible, en caso de ser necesario el analista de soporte en conjunto con el área de mantenimiento generan la orden de servicio de solicitar más combustible para recargar la planta.
- Para Detallar más ejemplos como solución a problemas de Hardware a servidores se podrán observar en el **(Anexo 4)**

10. MARCO GEOGRÁFICO

El Plan de Recuperación de Desastres está enfocado a la empresa Concesionaria para la operación y explotación del sistema de Recaudos y de control de flota en la ciudad de Barranquilla y su área Metropolitana, conformado por sus dos data center y las estaciones de que conforman las

paradas de buses de Transmetro de la Calle Murillo y la Carrera 46 de la ciudad de Barranquilla

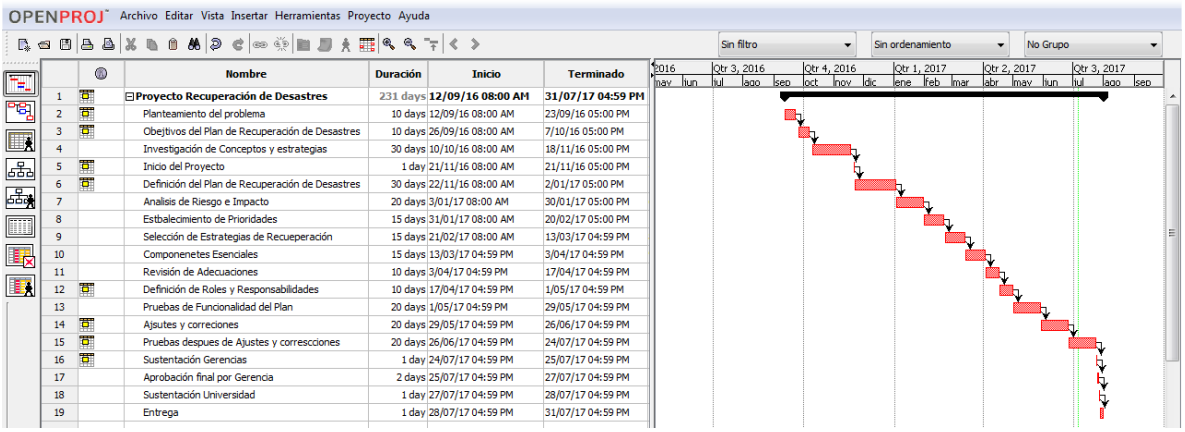
Figura No 15: *MAPA* - Rutas del Sistema integrado de Transporte Masivo
Fuente: Recaudos SIT Barranquilla S.A.S

11. CONCLUSIONES

- El Marco propuesto para la elaboración de un Plan de Recuperación de Desastres - **DRP**, deberá ser aprobado por la Junta Directiva (accionistas y dueños de la empresa) y el comité de Gerencia (Gerente General, Financiero, Técnico-Operativo y Directores de área) para que su aplicación y uso en las áreas de la compañía
- Se deberá emprender una campaña de concientizar a todos los colaboradores de la empresa sobre los aspectos de como beneficiara positivamente el plan de recuperación de desastres convendrá a la compañía
- El Plan de Recuperación de Desastres – **DRP,** Proporciona un marco de trabajo para construir una organización más resistente a desastres tecnológicos, con capacidad para responder de forma efectiva a los incidentes o desastres que le puedan ocurrir durante su operación diaria.
- El Plan de Recuperación de Desastres – **DRP** evitara que la empresa falle a los lineamientos del contrato de concesión y en caso de presentarse un incidente mayor o un desastre tecnológico, lograra recuperar su operación antes de incurrir en fallas a los acuerdos de niveles de servicio establecidos en el contrato.

12. CRONOGRAMA

El proyecto del diseño del plan de recuperación en caso de desastres para la plataforma informática de recaudos y control de flota de un sistema de transporte masivo de pasajeros tiene una duración aproximada de 210 días inicio desde el 12-09-2016 y finaliza el 31-07-2017



	Nombre	Duración	Inicio	Terminado
1	Proyecto Recuperación de Desastres	231 days	12/09/16 08:00 AM	31/07/17 04:59 PM
2	Planteamiento del problema	10 days	12/09/16 08:00 AM	23/09/16 05:00 PM
3	Obejtivos del Plan de Recuperación de Desastres	10 days	26/09/16 08:00 AM	7/10/16 05:00 PM
4	Investigación de Conceptos y estrategias	30 days	10/10/16 08:00 AM	18/11/16 05:00 PM
5	Inicio del Proyecto	1 day	21/11/16 08:00 AM	21/11/16 05:00 PM
6	Definición del Plan de Recuperación de Desastres	30 days	22/11/16 08:00 AM	2/01/17 05:00 PM
7	Analisis de Riesgo e Impacto	20 days	3/01/17 08:00 AM	30/01/17 05:00 PM
8	Estbalecimiento de Prioridades	15 days	31/01/17 08:00 AM	20/02/17 05:00 PM
9	Selección de Estrategias de Recueperación	15 days	21/02/17 08:00 AM	13/03/17 04:59 PM
10	Componenetes Esenciales	15 days	13/03/17 04:59 PM	3/04/17 04:59 PM
11	Revisión de Adecuaciones	10 days	3/04/17 04:59 PM	17/04/17 04:59 PM
12	Definición de Roles y Responsabilidades	10 days	17/04/17 04:59 PM	1/05/17 04:59 PM
13	Pruebas de Funcionalidad del Plan	20 days	1/05/17 04:59 PM	29/05/17 04:59 PM
14	Ajsutes y correciones	20 days	29/05/17 04:59 PM	26/06/17 04:59 PM
15	Pruebas despues de Ajustes y corresccciones	20 days	26/06/17 04:59 PM	24/07/17 04:59 PM
16	Sustentación Gerencias	1 day	24/07/17 04:59 PM	25/07/17 04:59 PM
17	Aprobación final por Gerencia	2 days	25/07/17 04:59 PM	27/07/17 04:59 PM
18	Sustentación Universidad	1 day	27/07/17 04:59 PM	28/07/17 04:59 PM
19	Entrega	1 day	28/07/17 04:59 PM	31/07/17 04:59 PM

Figura No 16: *CRONOGRAMA - Plan de Recuperación de Desastres – DRP*
Fuente: Elaboración Propia

13.REVISÓN BIBLIOGRAFÍA

13.1 REFERENCIAS

[1] **Recaudos SIT Barranquilla S.A.S.** Misión y Visión de la Empresa, http://www.sitbarranquilla.com/index.php/nuestra-empresa/mision-vision

[2] **Recaudos SIT Barranquilla S.A.S.** Misión y Visión de la Empresa, http://www.sitbarranquilla.com/index.php/nuestra-empresa/mision-vision

[3] **Contrato de concesión entre Transmetro S.A.S y Recaudos SIT Barranquilla S.A.S:** Contrato de concesión para la operación y explotación del sistema de recaudo y suministro del sistema de gestión y control de la operación del sistema Transmetro – ***Capitulo 20 – Multas***

[4] **Contrato de concesión entre Transmetro S.A.S y Recaudos SIT Barranquilla S.A.S:** Contrato de concesión para la operación y explotación del sistema de recaudo y suministro del sistema de gestión y control de la operación del sistema Transmetro **- ANEXO No. 6: NIVELES DE SERVICIO**

[5] **TECHTARGET:** proporciona estrategias tecnológicas para los profesionales de las TI. Ofrecen consejos, estrategias y mejores prácticas en el ámbito tecnológico que le ayudarán a simplificar y racionalizar sus operaciones. **http://searchdatacenter.techtarget.com/es/definicion/Que-es-Plan-de-Recuperacion-de-Desastres-DRP**

[6] ISACA. COBIT 5: Procesos Catalizadores, publicación que contiene una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de COBIT 5; **Proceso DSS04 Gestionar la continuidad**

[7] TECHTARGET: proporciona estrategias tecnológicas para los profesionales de las TI. Ofrecen consejos, estrategias y mejores prácticas en el ámbito tecnológico que le ayudarán a simplificar y racionalizar sus operaciones **http://searchdatacenter.techtarget.com/es/cronica/De-la-A-a-la-Z-plan-para-la-recuperacion-de-desastres-RD-TI**

[8] DRI: Disaster Recovery Institute; organización sin ánimo de lucro que proporciona formación a nivel internacional como organismo de certificación de profesionales para la Gestión de la Continuidad de Negocio

[9] Grupo Albe: Es una empresa de consultoría que cuenta con consultores e instructores que en sus servicios de consultoría a diseñado una metodología para implementar **DRP** *(Disaster Recovery Plan) (Plan de Recuperación de Desastres) a* proyectos de consultoría con sus clientes

[10] IBM: International Business Machines, empresa multinacional estadounidense de tecnología y consultoría con sede en Armonk, Nueva York. IBM fabrica y comercializa hardware y software para computadoras y ofrece servicios de infraestructura, alojamiento de Internet y consultoría en una amplia gama de áreas relacionadas con la informática.

[11] IBM Knowledge Center - Centro de conocimientos de IBM: Blogs de Especialistas de IBM donde aportan y comparten sus experiencias en diversas áreas de la Tecnología así como metodologías y ejemplos para un DRP. https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_61/rzarm/rzarmrcvrypl.htm

[12] VMware: Es una compañía que proporciona software de virtualización disponible para ordenadores compatibles X86. También es una filial de EMC Corporation (propiedad a su vez de Dell Inc)

[13] Blogs Vmware: Blogs de Especialistas de VMware donde comparten sus experiencias en diversas áreas de la Tecnología de la virtualización así como ejemplos para un DRP **https://blogs.vmware.com/latam/2015/08/recuperacion-de-desastres-informaticos-disene-deseando-lo-mejor-en-funcion-de-esperar-lo-peor.html#respond**

[14] BOSTON Computing Network: Empresa de servicios técnicos de outsourcing, asus clientes, dentro de los servcios que propone esta Web Hosting, Consultoría en Tecnologías Informáticas y desarrollo web. https://www.bostoncomputing.net/consultation/databackup/statistics/

[15] Norma ISO 22301 –Gestión de la continuidad de Negocio: es una norma internacional de gestión de **continuidad de negocio**. Esta norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando.

[16] ITIL, (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de Información es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, también da descripciones detalladas de un conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de T.I.

[17] Estándar AS/NZS 4360: Comité de Normas Conjuntas Australia / Nueva Zelanda AS /NZS 4360 Gestión de Riesgos

ANEXOS

1. GLOSARIO DE TÉRMINOS

Dispositivos Plataforma tecnológica del sistema de Transporte Masivo

Ítem	Nombre	Descripción
1	**CATI**	Cargador Automático de Tarjetas Inteligentes
2	PDA	Agenda Digital Portable
3	TCA	Terminal de Carga Asistida
4	BCA	Barrera de control de Acceso
5	TCS	Terminal de Consulta de Saldo
6	UCD	Unidad de consolidación de Datos
7	Validador	Modulo lector de Tarjeta
8	SAM	Load Security Module (Modulo de acceso Seguro)
9	B-SAM	Modulo de Acceso seguro en Barrera de control
10	L-SAM	Modulo de Acceso seguro en Terminales de Venta
11	MSM	Modulo Maestro de Seguridad
12	S-SM	Modulo de Seguridad para servidor de Estación

2. SIGLAS

ítem	Nombre	Descripción
1	**DRP**	**DRP** *(Disaster Recovery Plan) (Plan de Recuperación de Desastres)*
2	**SAN**	**SAN** (Storage Area Network) (Red de Área de Almacenamiento)
3	**PFA**	Análisis predictivo de fallas
4	**TI**	Tecnología de Información
5	**ITIL**	(Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de Información
6	**ISO 22301**	Estándar para el Sistema de Gestión de Seguridad de la Información
7	**SGCN**	**Sistema de Gestión de la Continuidad de Negocio**
8	**BIA**	Analisis de Impacto de Negocio - BIA
9	**SLA**	Acuerdo de Nivel de Servicio
10	**OLA**	Acuerdo de Nivel Operacional
		Significados e Infraestructuras de Hardware y Software
11	**Cluster**	Este tipo de sistemas se basa en la unión de varios servidores que trabajan como si de uno sólo se tratase. Los sistemas cluster han evolucionado mucho desde su primera aparición, ahora se pueden crear distintos tipos de clusters, en función de lo que se necesite:

3. Archivos Anexos

Archivos Anexos al documento principal como guía de consulta

Ítem	Nombre	Descripción	Archivo
1	**Anexo 1**	Presentación DRP	Presentación DRP.pdf
2	**Anexo 2**	Analisis de Riesgos	Analisis de Riesgos.pdf
3	**Anexo 3**	Matriz de Asignación de Responsabilidades RACI	Matriz RACI.pdf
4	**Anexo 4**	Plan de Recuperación de Desastres propuesto	DRP_Propuesto.pdf